PCT/JP99/05689

14.10.99

EKJ

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年１１月 ４日

出 願 番 号
Application Number: 平成１０年特許願第３１３０２０号

出 願 人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a)OR(b)

１９９９年 ８月２４日

特許庁長官
Commissioner,
Patent Office 伊佐山建志

出証番号 出証特平１１－３０５９１５１

【書類名】　特許願

【整理番号】　9800814907

【提出日】　平成10年11月 4日

【あて先】　特許庁長官殿

【国際特許分類】　H04K 1/00

【発明の名称】　情報処理装置および方法、提供媒体、並びに情報記憶媒体

【請求項の数】　13

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　石橋　義人

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　浅野　智之

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100082131

【弁理士】

【氏名又は名称】　稲本　義雄

【電話番号】　03-3369-6479

【手数料の表示】

【予納台帳番号】　032089

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708842

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置および方法、提供媒体、並びに情報記憶媒体

【特許請求の範囲】

【請求項１】　暗号化されている情報を復号して利用する情報処理装置において、

前記情報の使用の許諾条件を示す情報を生成する許諾条件情報生成手段と、

前記許諾条件を示す情報の認証情報を生成する認証情報生成手段と、

前記認証情報を記憶する記憶手段と

を備えることを特徴とする情報処理装置。

【請求項２】　前記記憶手段は、耐タンパー性を有する構造である

ことを特徴とする請求項１に記載の情報処理装置。

【請求項３】　暗号化されている情報を復号して利用する情報処理方法において、

前記情報の使用の許諾条件を示す情報を生成する許諾条件情報生成ステップと、

前記許諾条件を示す情報の認証情報を生成する認証情報生成ステップと、

前記認証情報を記憶する記憶ステップと

を含むことを特徴とする情報処理方法。

【請求項４】　暗号化されている情報を復号して利用する情報処理装置に、

前記情報の使用の許諾条件を示す情報を生成する許諾条件情報生成ステップと、

前記許諾条件を示す情報の認証情報を生成する認証情報生成ステップと、

前記認証情報を記憶する記憶ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項５】　装着された情報記憶媒体に情報を記憶させて利用する情報処理装置において、

前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段と、

前記認証情報を記憶する記憶手段と、

前記関連情報から、他の認証情報を生成し、前記記憶手段が記憶している前記認証情報との一致を検証する検証手段と、

前記情報記憶媒体と相互認証する相互認証手段と

を備えることを特徴とする情報処理装置。

【請求項６】　前記情報を暗号化する暗号化手段

を更に備えることを特徴とする請求項５に記載の情報処理装置。

【請求項７】　前記認証情報を暗号化する暗号化手段

を更に備えることを特徴とする請求項５に記載の情報処理装置。

【請求項８】　前記記憶手段が記憶する暗号化されている前記認証情報を復号する復号手段

を更に備えることを特徴とする請求項７に記載の情報処理装置。

【請求項９】　装着された情報記憶媒体に情報を記憶させて利用する情報処理装置の情報処理方法において、

前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成ステップと、

前記認証情報を記憶する記憶ステップと、

前記関連情報から、他の認証情報を生成し、前記記憶ステップで記憶した前記認証情報との一致を検証する検証ステップと、

前記情報記憶媒体と相互認証する相互認証ステップと

を含むことを特徴とする情報処理方法。

【請求項１０】　装着された情報記憶媒体に情報を記憶させて利用する情報処理装置に、

前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成ステップと、

前記認証情報を記憶する記憶ステップと、

前記関連情報から、他の認証情報を生成し、前記記憶ステップで記憶した前記認証情報との一致を検証する検証ステップと、

前記情報記憶媒体と相互認証する相互認証ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項１１】　暗号化された情報を記憶し、情報処理装置に装着される情報記憶媒体において、

前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段と、

前記認証情報を記憶する記憶手段と、

前記関連情報から、他の認証情報を生成し、前記記憶手段が記憶している前記認証情報との一致を検証する検証手段と、

前記情報処理装置と相互認証する相互認証手段と

を備えることを特徴とする情報記憶媒体。

【請求項１２】　前記認証情報を暗号化する暗号化手段

を更に備えることを特徴とする請求項１１に記載の情報記憶媒体。

【請求項１３】　前記記憶手段が記憶する暗号化されている前記認証情報を復号する復号手段

を更に備えることを特徴とする請求項１１に記載の情報記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置および方法、提供媒体、並びに情報記憶媒体に関し、特に、暗号化された情報を復号する情報処理装置および方法、提供媒体、並びに情報記憶媒体に関する。

【０００２】

【従来の技術】

音楽などの情報を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザは、その情報処理装置で情報を復号して、再生するシステムがある。ユーザは、例えば再生のみの利用、または５回の再生など、情報毎に利用内容を定め、情報を利用することができる。

【０００３】

【発明が解決しようとする課題】

しかし、利用内容を示す情報を書き換えることにより、所定の料金を支払わずに、例えば、再生の回数の制限を解除する、または、再生のみからコピーも可能とするなど、利用内容を変更することができる。

【０００４】

本発明はこのような状況に鑑みてなされたものであり、利用内容を示す情報の書き換えを検知し、対応できるようにすることを目的とする。

【０００５】

【課題を解決するための手段】

請求項１に記載の情報処理装置は、情報の使用の許諾条件を示す情報を生成する許諾条件情報生成手段と、許諾条件を示す情報の認証情報を生成する認証情報生成手段と、認証情報を記憶する記憶手段とを備えることを特徴とする。

【０００６】

請求項３に記載の情報処理方法は、情報の使用の許諾条件を示す情報を生成する許諾条件情報生成ステップと、許諾条件を示す情報の認証情報を生成する認証情報生成ステップと、認証情報を記憶する記憶ステップとを含むことを特徴とする。

【０００７】

請求項４に記載の提供媒体は、情報処理装置に、情報の使用の許諾条件を示す情報を生成する許諾条件情報生成ステップと、許諾条件を示す情報の認証情報を生成する認証情報生成ステップと、認証情報を記憶する記憶ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【０００８】

請求項５に記載の情報処理装置は、情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段と、認証情報を記憶する記憶手段と、関連情報から、他の認証情報を生成し、記憶手段が記憶している認証情報との一致を検証する検証手段と、情報記憶媒体と相互認証する相互認証手段とを備えることを特

徴とする。

【０００９】

請求項９に記載の情報処理方法は、情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成ステップと、認証情報を記憶する記憶ステップと、関連情報から、他の認証情報を生成し、記憶ステップで記憶した認証情報との一致を検証する検証ステップと、情報記憶媒体と相互認証する相互認証ステップとを含むことを特徴とする。

【００１０】

請求項１０に記載の提供媒体は、情報処理装置に、情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成ステップと、認証情報を記憶する記憶ステップと、関連情報から、他の認証情報を生成し、記憶ステップで記憶した認証情報との一致を検証する検証ステップと、情報記憶媒体と相互認証する相互認証ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【００１１】

請求項１１に記載の情報記憶媒体は、情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段と、認証情報を記憶する記憶手段と、関連情報から、他の認証情報を生成し、記憶手段が記憶している認証情報との一致を検証する検証手段と、情報処理装置と相互認証する相互認証手段とを備えることを特徴とする情報記憶媒体。

【００１２】

請求項１に記載の情報処理装置、請求項３に記載の情報処理方法、および請求項４に記載の提供媒体においては、情報の使用の許諾条件を示す情報を生成し、許諾条件を示す情報の認証情報を生成し、認証情報を記憶する。

【００１３】

~~請求項５に記載の情報処理装置、請求項９に記載の情報処理方法、および請求~~項１０に記載の提供媒体においては、情報の利用のときに必要な関連情報の認証情報を生成し、認証情報を記憶し、関連情報から、他の認証情報を生成し、記憶している認証情報との一致を検証し、情報記憶媒体と相互認証する。

【００１４】

請求項１１に記載の情報記憶媒体においては、認証情報生成手段が、情報の利用のときに必要な関連情報の認証情報を生成し、記憶手段認が証情報を記憶し、検証手段が、関連情報から、他の認証情報を生成し、記憶手段が記憶している認証情報との一致を検証し、相互認証手段が、情報処理装置と相互認証する。

【００１５】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００１６】

すなわち、請求項１に記載の情報処理装置は、情報の使用の許諾条件を示す情報を生成する許諾条件情報生成手段（例えば、図１０の課金処理モジュール７２）と、許諾条件を示す情報の認証情報を生成する認証情報生成手段（例えば、図１０の復号／暗号化モジュール７４）と、認証情報を記憶する記憶手段（例えば、図１０の記憶モジュール７３）とを備えることを特徴とする。

【００１７】

請求項５に記載の情報処理装置は、情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段（例えば、図３０の復号／暗号化モジュール７４）と、認証情報を記憶する記憶手段（例えば、図３０の記憶モジュール７３）と、関連情報から、他の認証情報を生成し、記憶手段が記憶している認証情報との一致を検証する検証手段（例えば、図３０のデータ検査モジュール１１４）と、情報記憶媒体と相互認証する相互認証手段（例えば、図３０の相互認証モジュール７１）とを備えることを特徴とする。

【００１８】

請求項１１に記載の情報記憶媒体は、情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段（例えば、図３０のデータ検査部１３８）と

、認証情報を記憶する記憶手段（例えば、図３０の記憶部１３５）と、関連情報から、他の認証情報を生成し、記憶手段が記憶している認証情報との一致を検証する検証手段（例えば、図３０のデータ検査部１３８）と、情報処理装置と相互認証する相互認証手段（例えば、図３０の相互認証部１３３）とを備えることを特徴とする情報記憶媒体。

【００１９】

図１は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。このシステムでユーザに配信されるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。EMDサービスセンタ１は、コンテンツプロバイダ２、ユーザホームネットワーク５等に配送用鍵Ｋｄを送信し、ユーザホームネットワーク５から、コンテンツの利用に応じた課金情報等を受信し、利用料金を精算し、コンテンツプロバイダ２およびサービスプロバイダ３への利益分配の処理を行う。

【００２０】

コンテンツプロバイダ２は、デジタル化されたコンテンツを有し、自己のコンテンツであることを証明するためのウォータマーク（電子透かし）をコンテンツに挿入し、コンテンツを圧縮し、および暗号化し、所定の情報を付加して、サービスプロバイダ３に送信する。

【００２１】

サービスプロバイダ３は、専用のケーブルネットワーク、インターネット、または衛星などから構成されるネットワーク４を介して、コンテンツプロバイダ２から供給されたコンテンツに価格を付して、ユーザホームネットワーク５に送信する。

【００２２】

ユーザホームネットワーク５は、サービスプロバイダ３から価格を付して送付されたコンテンツを入手し、コンテンツを復号、再生して利用するとともに課金処理を実行する。課金処理により得られた課金情報は、ユーザホームネットワーク５が配送用鍵ＫｄをEMDサービスセンタ１から入手する際、EMDサービスセンタ

１に送信される。

【００２３】

図２は、EMDサービスセンタ１の機能の構成を示すブロック図である。サービスプロバイダ管理部１１は、サービスプロバイダ３に利益分配の情報を供給するとともに、コンテンツプロバイダ２から供給されるコンテンツに付される情報（取扱方針）が暗号化されている場合、サービスプロバイダ３に配送用鍵Ｋｄを送信する。コンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信するとともに、利益分配の情報を供給する。著作権管理部１３は、ユーザホームネットワーク５のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC(Japanese Society for Rights of Authors,Composers and Publishers:日本音楽著作権協会)に送信する。鍵サーバ１４は、配送用鍵Ｋｄを記憶しており、コンテンツプロバイダ管理部１２、またはユーザ管理部１８等を介して、配送用鍵Ｋｄをコンテンツプロバイダ２、またはユーザホームネットワーク５等に供給する。ユーザ管理部１８は、ユーザホームネットワーク５のコンテンツの利用の実績を示す情報である課金情報、そのコンテンツに対応する価格情報、およびそのコンテンツに対応する取扱方針を入力し、経歴データ管理部１５に記憶させる。

【００２４】

EMDサービスセンタ１からコンテンツプロバイダ２およびユーザホームネットワーク５を構成するレシーバ５１（図１０で後述する）への、配送用鍵Ｋｄの定期的な送信の例について、図３乃至図６を参照に説明する。図３は、コンテンツプロバイダ２がコンテンツの提供を開始し、ユーザホームネットワーク５を構成するレシーバ５がコンテンツの利用を開始する、１９９８年１月における、EMDサービスセンタ１が有する配送用鍵Ｋｄ、コンテンツプロバイダ２が有する配送用鍵Ｋｄ、およびレシーバ５１が有する配送用鍵Ｋｄを示す図である。

【００２５】

図３の例において、配送用鍵Ｋｄは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である”ａａａａａａａａ”の値を有するバージョン１である配送用鍵Ｋｄは、１９９８年１月１日から１９９８年

１月３１日まで使用可能（すなわち、１９９８年１月１日から１９９８年１月３１日の期間にサービスプロバイダ３がユーザホームネットワーク５に配布するコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン１である配送用鍵Ｋｄで暗号化されている）であり、所定のビット数の乱数である”ｂｂｂｂｂｂｂｂ”の値を有するバージョン２である配送用鍵Ｋｄは、１９９８年２月１日から１９９８年２月２８日まで使用可能（すなわち、その期間にサービスプロバイダ３がユーザホームネットワーク５に配布するコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン１である配送用鍵Ｋｄで暗号化されている）である。同様に、バージョン３である配送用鍵Ｋｄは、１９９８年３月中に使用可能であり、バージョン４である配送用鍵Ｋｄは、１９９８年４月中に使用可能であり、バージョン５である配送用鍵Ｋｄは、１９９８年５月中に使用可能であり、バージョン６である配送用鍵Ｋｄは、１９９８年６月中に使用可能である。

【００２６】

コンテンツプロバイダ２がコンテンツの提供を開始するに先立ち、EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年１月から１９９８年６月まで利用可能な、バージョン１乃至バージョン６の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、記憶する。６月分の配送用鍵Ｋｄを記憶するのは、コンテンツプロバイダ２は、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

【００２７】

また、レシーバ５１がコンテンツの利用を開始するに先立ち、EMDサービスセンタ１は、レシーバ５１に、１９９８年１月から１９９８年３月まで、利用可能なバージョン１乃至バージョン３である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、記憶する。３月分の配送用鍵Ｋｄを記憶するのは、レシーバ５１が、EMDサービスセンタ１に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ１への接続の頻度を低くし、ユーザホームネットワーク５の負荷を低減するためである。

【００２８】

１９９８年1月１日から１９９８年１月３１日の期間には、バージョン１である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００２９】

１９９８年2月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図４で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年２月から１９９８年７月まで利用可能な、バージョン２乃至バージョン７の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年２月から１９９８年４月まで、利用可能なバージョン２乃至バージョン４である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Ｋｄを利用できるようにするためである。

【００３０】

１９９８年2月１日から１９９８年２月２８日の期間には、バージョン２である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３１】

１９９８年3月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図５で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年３月から１９９８年８月まで利用可能な、バージョン３乃至バージョン８の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセ

ンタ１は、レシーバ５１に、１９９８年３月から１９９８年５月まで、利用可能なバージョン３乃至バージョン５である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵ＫｄおよびバージョンＮ２である配送用鍵Ｋｄをそのまま記憶する。

【００３２】

１９９８年３月１日から１９９８年３月３１日の期間には、バージョン３である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３３】

１９９８年４月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図６で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年４月から１９９８年９月まで利用可能な、バージョン４乃至バージョン９の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年４月から１９９８年６月まで、利用可能なバージョン３乃至バージョン５である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄ、バージョン２である配送用鍵Ｋｄ、およびバージョン３である配送用鍵Ｋｄをそのまま記憶する。

【００３４】

１９９８年４月１日から１９９８年４月３０日の期間には、バージョン４である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３５】

利益分配部１６は、経歴データ管理部１５から供給された、課金情報、価格情

報、および取扱方針に基づき、EMDサービスセンタ１、コンテンツプロバイダ２、およびサービスプロバイダ３の利益を算出する。相互認証部１７は、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の所定の機器と後述する相互認証を実行する。

【００３６】

ユーザ管理部１８は、ユーザ登録データベースを有し、ユーザホームネットワーク５の機器から登録の要求があったとき、ユーザ登録データベースを検索し、その記録内容に応じて、その機器を登録したり、または登録を拒絶する等の処理を実行する。ユーザホームネットワーク５がEMDサービスセンタ１と接続が可能な機能を有する複数の機器から構成されているとき、ユーザ管理部１８は、登録が可能か否かの判定の処理の結果に対応して、決済をする機器を指定し、さらに、コンテンツの利用条件を規定した登録リストをユーザホームネットワーク５の所定の機器に送信する。

【００３７】

図７に示すユーザ登録データベースの例は、ユーザホームネットワーク５の機器の機器固有の６４ビットからなるID（Identification Data）を記録し、そのIDに対応して（すなわち、そのIDを有する機器毎に）、決済処理が可能か否か、登録が可能か否か、EMDサービスセンタ１と接続が可能か否か等の情報を記録する。ユーザ登録データベースに記録された登録が可能か否かの情報は、決済機関（例えば、銀行）、またはサービスプロバイダ３などから供給される料金の未払い、不正処理等の情報を基に、所定の時間間隔で更新される。登録が不可と記録されたIDを有する機器の登録の要求に対して、ユーザ管理部１８は、その登録を拒否し、登録を拒否された機器は、以後、このシステムのコンテンツを利用できない。

【００３８】

ユーザ登録データベースに記録された決済処理が可能か否かの情報は、その機器が、決済可能か否かを示す。ユーザホームネットワーク５が、コンテンツの再生またはコピーなどの利用が可能な複数の機器で構成されているとき、その中の決済処理が可能である１台の機器は、EMDサービスセンタ１に、ユーザホームネ

ットワーク５のEMDサービスセンタ１に登録されている全ての機器の、課金情報、価格情報、および取扱方針を出力する。ユーザ登録データベースに記録されたEMDサービスセンタ１と接続が可能か否かの情報は、その機器が、EMDサービスセンタ１と接続が可能であるか否かを示し、接続ができないと記録された機器は、ユーザホームネットワーク５の他の機器を介して、EMDサービスセンタ１に、課金情報等を出力する。

【００３９】

また、ユーザ管理部１８は、ユーザホームネットワーク５の機器から課金情報、価格情報、および取扱方針が供給され、その情報を経歴データ管理部１５に出力し、さらに、所定の処理（タイミング）で、ユーザホームネットワーク５の機器に、配送用鍵Ｋｄを供給する。

【００４０】

課金請求部１９は、経歴データ管理部１５から供給された、課金情報、価格情報、および取扱方針に基づき、ユーザへの課金を算出し、その結果を、出納部２０に供給する。出納部２０は、ユーザ、コンテンツプロバイダ２、およびサービスプロバイダ３への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。監査部２１は、ユーザホームネットワーク５の機器から供給された課金情報、価格情報、および取扱方針の正当性（すなわち、不正をしていないか）を監査する。

【００４１】

図８は、コンテンツプロバイダ２の機能の構成を示すブロック図である。コンテンツサーバ３１は、ユーザに供給するコンテンツを記憶し、ウォータマーク付加部３２に供給する。ウォータマーク付加部３２は、コンテンツサーバ３１から供給されたコンテンツにウォータマークを付加し、圧縮部３３に供給する。圧縮部３３は、ウォータマーク付加部３２から供給されたコンテンツを、ATRAC2(Adaptive Transform Acoustic Coding 2)（商標）等の方式で圧縮し、暗号化部３４に供給する。暗号化部３４は、圧縮部３３で圧縮されたコンテンツを、乱数発生部３５から供給された乱数を鍵（以下、この乱数をコンテンツ鍵Ｋｃｏと称する）として、DES(Data Encryption Standard)などの共通鍵暗号方式で暗号化し、

その結果をセキュアコンテナ作成部３８に出力する。

【００４２】

乱数発生部３５は、コンテンツ鍵Ｋｃｏとなる所定のビット数の乱数を暗号化部３４および暗号化部３６に供給する。暗号化部３６は、コンテンツ鍵ＫｃｏをEMDサービスセンタ１から供給された配送用鍵Ｋｄを使用して、DESなどの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

【００４３】

DESは、５６ビットの共通鍵を用い、平文の６４ビットを１ブロックとして処理する暗号方式である。DESの処理は、平文を撹拌し、暗号文に変換する部分（データ撹拌部）と、データ撹拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ撹拌部の基本的な処理を簡単に説明する。

【００４４】

まず、平文の６４ビットは、上位３２ビットのH_0、および下位３２ビットのL_0に分割される。鍵処理部から供給された４８ビットの拡大鍵K_1、および下位３２ビットのL_0を入力とし、下位３２ビットのL_0を撹拌したＦ関数の出力が算出される。Ｆ関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の２種類の基本変換から構成されている。次に、上位３２ビットのH_0と、Ｆ関数の出力が排他的論理和され、その結果はL_1とされる。L_0は、H_1とされる。

【００４５】

上位３２ビットのH_0および下位３２ビットのL_0を基に、以上の処理を１６回繰り返し、得られた上位３２ビットのH_{16}および下位３２ビットのL_{16}が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【００４６】

ポリシー記憶部３７は、コンテンツの取扱方針（ポリシー）を記憶し、暗号化されるコンテンツに対応して、取扱方針をセキュアコンテナ作成部３８に出力する。セキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコ

ンテンツ鍵Ｋｃｏ、取扱方針、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、および取扱方針のハッシュ値をとり作成された署名、さらにコンテンツプロバイダ２の公開鍵Ｋｐｃｐを含む証明書から構成されるコンテンツプロバイダセキュアコンテナを作成し、サービスプロバイダ３に供給する。相互認証部３９は、EMDサービスセンタ１から配送用鍵Ｋｄの供給を受けるのに先立ち、EMDサービスセンタ１と相互認証し、また、サービスプロバイダ３へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ３と相互認証する。

【００４７】

署名は、データまたは後述する証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【００４８】

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【００４９】

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4, MD5, SHA-1などが用いられる。

【００５０】

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を

使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【００５１】

公開鍵暗号の中で代表的なRSA（Rivest-Shamir-Adleman）暗号を、簡単に説明する。まず、２つの十分に大きな素数であるpおよびqを求め、さらにpとqの積であるｎを求める。(p-1)と(q-1)の最小公倍数Lを算出し、更に、３以上L未満で、かつ、Ｌと互いに素な数eを求める（すなわち、eとLを共通に割り切れる数は、１のみである）。

【００５２】

次に、Lを法とする乗算に関するeの乗法逆元dを求める。すなわち、d，e、およびLの間には、ed=1 mod Lが成立し、dはユークリッドの互除法で算出できる。このとき、nとeが公開鍵とされ、p,q,およびdが、秘密鍵とされる。

【００５３】

暗号文Cは、平文Mから、式（１）の処理で算出される。

C=M^e mod n　　(1)

【００５４】

暗号文Cは、式（２）の処理で平文Mに、復号される。

M=C^d mod n　　（２）

【００５５】

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式（３）が成立するからである。

M=C^d=(M^e)^d=M^(ed) mod n　　（３）

【００５６】

秘密鍵pとqを知っているならば、公開鍵eから秘密鍵dは算出できるが、公開鍵nの素因数分解が計算量的に困難な程度に公開鍵nの桁数を大きくすれば、公開鍵nを知るだけでは、公開鍵eから秘密鍵dは計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とす

ることができる。

【００５７】

また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線y^2=x^3+ax+b上の、ある点をBとする。楕円曲線上の点の加算を定義し、nBは、Bをn回加算した結果を表す。同様に、減算も定義する。BとnBからnを算出することは、困難であることが証明されている。BとnBを公開鍵とし、nを秘密鍵とする。乱数rを用いて、暗号文C1およびC2は、平文Mから、公開鍵で式（４）および式（５）の処理で算出される。

C1=M+rnB　（４）

C2=rB　（５）

【００５８】

暗号文C1およびC2は、式（６）の処理で平文Mに、復号される。

M=C1-nC2　（６）

【００５９】

復号できるのは、秘密鍵nを有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【００６０】

図９は、サービスプロバイダ３の機能の構成を示すブロック図である。コンテンツサーバ４１は、コンテンツプロバイダ２から供給された、暗号化されているコンテンツを記憶し、セキュアコンテナ作成部４４に供給する。値付け部４２は、コンテンツに対応した取扱方針を基に、価格情報を作成し、セキュアコンテナ作成部４４に供給する。ポリシー記憶部４３は、コンテンツプロバイダ２から供給された、コンテンツの取扱方針を記憶し、セキュアコンテナ作成部４４に供給する。相互認証部４５は、コンテンツプロバイダ２からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ２と相互認証し、また、ユーザホームネットワーク５へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク５と相互認証する。また、コンテンツプロバイダ２が取扱方針を配送用鍵Ｋｄで暗号化して供給する場合、相互

認証部４５は、EMDサービスセンタ１から配送用鍵Ｋｄの供給を受け付けるのに先立ち、EMDサービスセンタ１と相互認証する。

【００６１】

図１０は、ユーザホームネットワーク５の構成を示すブロック図である。レシーバ５１は、ネットワーク４を介して、サービスプロバイダ３からコンテンツを含んだサービスプロバイダセキュアコンテナを受信し、コンテンツを復号および伸張し、再生する。

【００６２】

通信部６１は、ネットワーク４を介してサービスプロバイダ３、またはEMDサービスセンタ１と通信し、所定の情報を受信し、または送信する。SAM(Secure Application Module)６２は、サービスプロバイダ３、またはEMDサービスセンタ１と相互認証し、コンテンツの暗号を復号し、またはコンテンツを暗号化し、さらに配送用鍵Ｋｄ等を記憶する。伸張部６３は、コンテンツの暗号を復号し、ATRAC2方式で伸張し、さらに所定のウォータマークをコンテンツに挿入する。IC（Integrated Circuit）カードインターフェース６４は、SAM６２からの信号を所定の形式に変更し、レシーバ５１に装着されたICカード５５に出力し、また、ICカード５５からの信号を所定の形式に変更し、SAM６２に出力する。

【００６３】

サービスプロバイダ３、またはEMDサービスセンタ１と相互認証し、課金処理を実行し、コンテンツ鍵Ｋｃｏを復号および暗号化し、さらに使用許諾条件情報等の所定のデータを記憶するSAM６２は、相互認証モジュール７１、課金モジュール７２、記憶モジュール７３、および復号／暗号化モジュール７４から構成される。このSAM６２は、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有する。

【００６４】

相互認証モジュール７１は、サービスプロバイダ３、またはEMDサービスセンタ１との相互認証を実行し、必要に応じて、一時鍵Ｋｔｅｍｐ（セッション鍵）

を復号／暗号化モジュール７４に供給する。課金処理モジュール７２は、サービスプロバイダ３から受信したサービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報（並びに、場合によっては、取扱制御情報）から、使用許諾条件情報および課金情報を生成し、記憶モジュール７３またはHDD(Hard Disk Drive)５２に出力する。記憶モジュール７３は、課金処理モジュール７２または復号／暗号化モジュール７４から供給された課金情報、および配送用鍵Ｋｄ等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送用鍵Ｋｄ等のデータを供給する。

【００６５】

復号／暗号化モジュール７４は、復号ユニット９１、乱数発生ユニット９２、および暗号化ユニット９３から構成される。復号ユニット９１は、暗号化されたコンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、暗号化ユニット９３に出力する。乱数発生ユニット９２は、所定の桁数の乱数を発生し、保存用鍵Ｋｓａｖｅとして暗号化ユニット９３および記憶モジュール７３に出力する。ただし、一度生成して保持している場合、生成の必要はない。暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを、再度、保存用鍵Ｋｓａｖｅで暗号化し、HDD５２に出力する。暗号化ユニット９３は、コンテンツ鍵Ｋｃｏを伸張部６３に送信するとき、コンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで暗号化する。

【００６６】

コンテンツを復号し、伸張し、所定のウォータマークを付加する伸張部６３は、相互認証モジュール７５、復号モジュール７６、復号モジュール７７、伸張モジュール７８、およびウォータマーク付加モジュール７９から構成される。相互認証モジュール７５は、SAM６２と相互認証し、一時鍵Ｋｔｅｍｐを復号モジュール７６に出力する。復号モジュール７６は、SAM６２から出力され、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、復号モジュール７７に出力する。復号モジュール７７は、HDD５２に記録されたコンテンツをコンテンツ鍵Ｋｃｏで復号し、伸張モジュール７８に出力する。伸張モジュール７８は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォータマーク付加モジュール７９に出力する。ウォータマーク付加モジュール７９

は、コンテンツにレシーバ５１を特定する所定のウォータマークを挿入し、レコーダ５３に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【００６７】

HDD５２は、サービスプロバイダ３から供給されたコンテンツを記録する。装着された光ディスク（図示せず）にサービスプロバイダ３から供給されたコンテンツを記録し、再生するレコーダ５３は、記録再生部６５、SAM６６、および伸張部６７から構成される。記録再生部６５は、光ディスクが装着され、その光ディスクにコンテンツを記録し、再生する。SAM６６は、SAM６２と同じ機能を有し、その説明は省略する。伸張部６７は、伸張部６３と同じ機能を有し、その説明は省略する。MD(Mini Disk:商標)ドライブ５４は、装着された図示せぬMDにサービスプロバイダ３から供給されたコンテンツを記録し、再生する。

【００６８】

ICカード５５は、レシーバ５１に装着され、記憶モジュール７３に記憶された配送用鍵Ｋｄおよび機器のIDなどの所定のデータを記憶する。例えば、新たなレシーバ５１を購入し、今まで使用していたレシーバ５１と入れ替えて使用する場合、まず、ユーザは、ICカード５５に、今まで使用していたレシーバ５１の記憶モジュール７３に記憶されていた配送用鍵Ｋｄなどの所定のデータを記憶させる。次に、ユーザは、そのICカード５５を新たなレシーバ５１に装着し、そのレシーバ５１を操作して、EMDサービスセンタ１のユーザ管理部１８にその新たなレシーバ５１を登録する。EMDサービスセンタ１のユーザ管理部１８は、ICカード５５に記憶されていたデータ（今まで使用していたレシーバ５１のIDなど）を基に、ユーザ管理部１８が保持しているデータベースから、ユーザの氏名、使用料の払い込みに使用するクレジットカードの番号などのデータを検索し、そのデータを基に、登録の処理を実行するので、ユーザは、面倒なデータを入力する必要がない。ICカード５５は、相互認証モジュール８０および記憶モジュール８１で構成される。相互認証モジュール８０は、SAM６２と相互認証する。記憶モジュール８１は、ICカードインターフェース６４を介して、SAM６２から供給されたデータを記憶し、記憶したデータをSAM６２に出力する。

【００６９】

図１１は、ユーザホームネットワーク５の他の構成例を示すブロック図である。この構成のレシーバ５１およびレコーダ５３は、図１０に示した伸張部６３および伸張部６７を省略した構成を有する。その代わり、レコーダ５３に接続されているデコーダ５６が、伸張部６３または伸張部６７と同じ機能を有する。その他の構成は、図１０における場合と同様である。

【００７０】

コンテンツを復号し、伸張し、ウォータマークを付加するデコーダ５６は、相互認証モジュール１０１、復号モジュール１０２、復号モジュール１０３、伸張モジュール１０４、およびウォータマーク付加モジュール１０５から構成される。相互認証モジュール１０１は、SAM６２またはSAM６６と相互認証し、一時鍵Ｋｔｅｍｐを復号モジュール１０２に出力する。復号モジュール１０２は、SAM６２から出力され、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、復号モジュール１０３に出力する。復号モジュール１０３は、HDD５２に記録されたコンテンツをコンテンツ鍵Ｋｃｏで復号し、伸張モジュール１０４に出力する。伸張モジュール１０４は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォータマーク付加モジュール１０５に出力する。ウォータマーク付加モジュール１０５は、コンテンツにデコーダ５６を特定する所定のウォータマークを挿入し、レコーダ５３に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【００７１】

図１２は、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の間で送受信される情報を説明する図である。コンテンツプロバイダ２は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および署名をコンテンツプロバイダセキュアコンテナ（その詳細は図１３を参照して後述する）に格納し、さらにコンテンツプロバイダセキュアコンテナにコンテンツプロバイダ２の証明書（その詳細は図１４を参照して後述する）を付して、サービスプロバイダ３に送信する。コンテンツプロバイダ２はまた、取扱方針、および署名にコンテンツプロバイダ２の証明

書を付して、EMDサービスセンタ１に送信する。

【００７２】

サービスプロバイダ３は、受信したコンテンツプロバイダセキュアコンテナに含まれる取扱方針を基に価格情報を生成し、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、価格情報、および署名をサービスプロバイダセキュアコンテナ（その詳細は図１５を参照して後述する）に格納し、さらにサービスプロバイダセキュアコンテナにサービスプロバイダ３の証明書（その詳細は図１６を参照して後述する）を付して、ユーザホームネットワーク５に送信する。サービスプロバイダ３はまた、価格情報、および署名にサービスプロバイダ３の証明書を付して、EMDサービスセンタ１に送信する。

【００７３】

ユーザホームネットワーク５は、受信したサービスプロバイダセキュアコンテナに含まれる取扱方針から使用許諾情報を生成し、使用許諾情報に沿って、コンテンツを利用する。ユーザホームネットワーク５において、コンテンツ鍵Ｋｃｏが復号されると、課金情報が生成される。課金情報は、所定のタイミングで、暗号化され、取扱方針と共に署名が付され、EMDサービスセンタ１に送信される。

【００７４】

EMDサービスセンタ１は、課金情報および取扱方針を基に使用料金を算出し、またEMDサービスセンタ１、コンテンツプロバイダ２、およびサービスプロバイダ３それぞれの利益を算出する。EMDサービスセンタ１は、さらに、コンテンツプロバイダ２から受信した取扱方針、サービスプロバイダ３から受信した価格情報、並びにユーザホームネットワーク５から受信した課金情報および取扱方針を比較し、サービスプロバイダ３またはユーザホームネットワーク５で取扱方針の改竄または不正な価格の付加等の不正がなかったか否かを監査する。

【００７５】

図１３は、コンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋ

ｄで暗号化されたコンテンツ鍵Ｋｃｏ、および取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ２の秘密鍵Ｋｓｃｐで暗号化したデータである。

【００７６】

図１４は、コンテンツプロバイダ２の証明書を説明する図である。コンテンツプロバイダ２の証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ２の名前、コンテンツプロバイダの公開鍵Ｋｐｃｐ、並びに署名を含む。署名は、証明書のバージョン番号、認証局がコンテンツプロバイダ２に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ２の名前、並びにコンテンツプロバイダの公開鍵Ｋｐｃｐにハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵Ｋｓｃａで暗号化したデータである。

【００７７】

図１５は、サービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、価格情報、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ３の秘密鍵Ｋｓｓｐで暗号化したデータである。

【００７８】

図１６は、サービスプロバイダ３の証明書を説明する図である。サービスプロバイダ３の証明書は、証明書のバージョン番号、認証局がサービスプロバイダ３に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ３の名前、サービスプロバイダの公開鍵Ｋｐｓｐ、並びに署名を含む。署名は、証明書のバージョン番号、認証局がサービスプロバイダ３に対し割り付ける証明書の通し番号、署名

に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ３の名前、サービスプロバイダの公開鍵Ｋｐｓｐにハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵Ｋｓｃａで暗号化したデータである。

【００７９】

図１７は、取扱方針、価格情報、および使用許諾条件情報を示す図である。コンテンツプロバイダ２が有する取扱方針（図１７（Ａ））は、コンテンツ毎に用意され、ユーザホームネットワーク５が利用可能な利用内容を示す。例えば、図１７（Ａ）の取り扱い方針は、ユーザホームネットワーク５がそのコンテンツを再生およびマルチコピーすることは許可するが、シングルコピーは許可しないことを示す。

【００８０】

図１８は、シングルコピーおよびマルチコピーを説明する図である。マルチコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、複数のコピーを作成することを言う。ただし、図１８（Ａ）に示すように、コピーを更にコピーすることはできない（許されない）。シングルコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、ただ１つのコピーを作成することを言う。シングルコピーの場合も、図１８（Ｂ）に示すように、コピーを更にコピーすることはできない（許されない）。

【００８１】

サービスプロバイダ３は、図１７（Ｂ）に示すように、コンテンツプロバイダ２からの取扱方針（図１７（Ａ））に価格情報を加える。例えば、図１７（Ｂ）の価格情報は、そのコンテンツを再生して利用するときの料金が１５０円で、マルチコピーして利用するときの利用料金が８０円であることを示す。図１７には、例示しないが、シングルコピーの価格情報は、コピーの１回当たりの使用料金を表し、例えば、３回のコピーの利用では、シングルコピーの使用料金の３倍の料金を支払う。マルチコピーまたはシングルコピーが許可されるコンテンツは、

使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合における、そのコンテンツに限られる。

【００８２】

ユーザホームネットワーク５は、サービスプロバイダ３から供給される取扱方針が示すコンテンツの利用可能な利用内容（図１７（Ｂ））から、ユーザが選択した、利用内容を示す使用許諾条件情報（図１７（Ｃ））を記憶する。例えば、図１７（Ｃ）の使用許諾条件情報は、そのコンテンツを再生して使用することができ、シングルコピーおよびマルチコピーができないことを示す。

【００８３】

図１９は、図１７の例と比較してコンテンツプロバイダ２が取扱方針に利益分配の情報を加え、サービスプロバイダ３が価格情報に利益分配の情報を加える場合の、取扱方針および価格情報を説明する図である。図１７に示す例に対して、図１９の例では、コンテンツプロバイダ２の利益が、コンテンツを再生して利用するとき７０円で、マルチコピーして利用するとき４０円であることを示す情報が、追加されている（図１９（Ａ））。更に、利益分配情報として、サービスプロバイダ３の利益が、コンテンツを再生して利用するとき６０円で、マルチコピーして利用するとき３０円であることが、追加されている（図１９（Ｂ））。価格は、図１７（Ａ）における場合と同様に、再生が１５０円、マルチコピーが４０円とされている。価格（例えば１５０円）からコンテンツプロバイダ２の利益（例えば７０円）およびサービスプロバイダ３の利益（例えば６０円）を差し引いた金額（例えば２０円）が、EMDサービスセンタ１の利益である。EMDサービスセンタ１は、ユーザホームネットワーク５のコンテンツの利用結果を示す課金情報（図１９（Ｃ））とともに、ユーザホームネットワーク５を介して、取扱方針、利益分配率、および価格情報を得ることで、コンテンツプロバイダ２、サービスプロバイダ３、およびEMDサービスセンタ１のそれぞれの利益を算出できる。

【００８４】

図２０は、コンテンツの再生の利用に、複数の形態が設定されているときの取扱方針、価格情報、および使用許諾条件情報を説明する図である。図２０（Ａ）の例では、サービスプロバイダ３において、取扱方針および価格情報として、コ

ンテンツの再生利用に、制限のない再生、回数制限（この例の場合、５回）のある再生、および期日制限（この例の場合、１９９８年１２月３１日まで）のある再生が設定されている。ユーザが、５回の回数制限のある再生を選択して、コンテンツを利用する場合、コンテンツを受け取り、まだ１度も再生していない状態では、図２０（Ｂ）に示すように、ユーザホームネットワーク５の使用許諾条件情報の回数制限に対応する値には、”５”が記録されている。この回数制限に対応する値は、ユーザホームネットワーク５において、コンテンツが再生（利用）される度にデクリメントされ、例えば、３回再生された後、その値は、図２０（Ｃ）に示すように”２”とされる。回数制限に対応する値が、”０”となった場合、ユーザホームネットワーク５は、それ以上、そのコンテンツを再生して利用することができない。

【００８５】

図２１は、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の間で送受信される情報の他の例を説明する図である。図１２に示した例に対して、図２１の例では、サービスプロバイダ３は、コンテンツプロバイダ２からの取扱方針を基に取扱制御情報を作成する。取扱制御情報は、コンテンツなどと共にサービスプロバイダセキュアコンテナに格納され、ユーザホームネットワーク５に送信され、EMDサービスセンタ１にも送信される。取扱制御情報は、更に、課金情報および取扱方針と共にユーザホームネットワーク５からEMDサービスセンタ１に送信される。

【００８６】

図２２は、図２１の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、取扱制御情報、価格情報、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、取扱制御情報、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ３の秘密鍵Ｋｓｓｐで暗号化したデータである。

【００８７】

図２３は、図２１の例の場合における、取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。図２３に示す例の場合、コンテンツプロバイダ２の取扱方針（図２３（Ａ））は、そのまま価格情報を付しても、取扱方針と対比して価格情報を参照できる形式を有しない。そこで、サービスプロバイダ３は、その取扱方針を基に、価格情報と対比して価格情報を参照できる形式を有する取扱制御情報を生成し、それに価格情報を付して、ユーザホームネットワーク５に送信する（図２３（Ｂ））。ユーザホームネットワークでは、送信を受けた情報から使用許諾条件情報（図２３（Ｃ））を生成する。図２３のコンテンツプロバイダ２は、図１２の場合に比較し、より小さいデータ量の取扱方針を記録すればよい利点がある。

【００８８】

図２４は、EMDサービスセンタ１、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の間で送受信されるコンテンツおよびコンテンツに付随する情報のさらに他の構成を説明する図である。図２１に示した例に対して、図２４の例では、取扱方針、取扱制御情報、価格情報、および課金情報は、公開鍵暗号により暗号化され、送信される。図２４のシステムは、図２１の例の場合に比較して、システムの外部からの攻撃に対し、安全性が向上する。

【００８９】

図２５は、図２４の例の場合のコンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、配送用鍵Ｋｄで暗号化された取扱方針、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、および配送用鍵Ｋｄで暗号化された取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ２の秘密鍵Ｋｓｃｐで暗号化したデータである。

【００９０】

図２６は、図２４の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、配送用鍵Ｋｄで暗号化された取扱方針、配送用鍵Ｋｄで暗号化された取扱制御情報、配送用鍵Ｋｄで暗号化された価格情報、および署名を含む。署名は、コンテンツ鍵Ｋｃｏで暗号化されたコンテンツ、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏ、配送用鍵Ｋｄで暗号化された取扱方針、配送用鍵Ｋｄで暗号化された取扱制御情報、および配送用鍵Ｋｄで暗号化された価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ３の秘密鍵Ｋｓｓｐで暗号化したデータである。

【００９１】

図２７は、EMDサービスセンタ１が、ユーザホームネットワーク５から課金情報を受信するときの動作を説明する図である。ユーザホームネットワーク５と相互認証した後、ユーザ管理部１８は、一時鍵Ｋｔｅｍｐを共有化し、鍵サーバ１４からの配送用鍵Ｋｄをユーザホームネットワーク５に送信する。ユーザホームネットワーク５は、共有化した一時鍵Ｋｔｅｍｐを用いて課金情報、および取扱方針等を暗号化し、EMDサービスセンタ１に送信する。ユーザ管理部１８はこれを受信する。ユーザ管理部１８は、受信した課金情報、および取扱方針等を経歴データ管理部１５および課金請求部１９に送信する。経歴データ管理部１５は決済を実行すると判定した場合、受信した課金情報を利益分配部１６に送信し、さらに、受信した課金情報および取扱方針等を課金請求部１９に送信する。利益分配部１６は、コンテンツプロバイダ２、サービスプロバイダ３、およびEMDサービスセンタ１自身に対する請求金額および支払金額を算出する。課金請求部１９は、ユーザの支払い金額を算出し、その情報を出納部２０に送信する。出納部２０は、図示せぬ外部の銀行等と通信し、決算処理を実行する。その際、ユーザの料金の未払い等の情報があれば、それらの情報は、課金請求部１９およびユーザ管理部１８に送信され、以後のユーザの登録処理時、または配送用鍵Ｋｄの送信処理時に参照される。

【００９２】

図２８は、EMDサービスセンタ１の利益分配処理の動作を説明する図である。経歴データ管理部１５は、ユーザのコンテンツの使用実績を示す課金情報、取扱方針、および価格データを利益分配部１６に送信する。利益分配部１６は、これらの情報を基に、コンテンツプロバイダ２、サービスプロバイダ３、およびEMDサービスセンタ１それぞれの利益を算出し、その結果をサービスプロバイダ管理部１１、コンテンツプロバイダ管理部１２、出納部２０、および著作権管理部１３に送信する。出納部２０は、図示せぬ外部の銀行等と通信し、決算処理を実行する。サービスプロバイダ管理部１１は、サービスプロバイダ３の利益の情報をサービスプロバイダ３に送信する。コンテンツプロバイダ管理部１２は、コンテンツプロバイダ２の利益の情報をコンテンツプロバイダ２に送信する。監査部２１は、ユーザホームネットワーク５の機器から供給された課金情報、価格情報、および取扱方針の正当性を監査する。

【００９３】

図２９は、EMDサービスセンタ１の、コンテンツの利用実績の情報をJASRACに送信する処理の動作を説明する図である。経歴データ管理部１５は、ユーザのコンテンツの使用実績を示す課金情報を著作権管理部１３および利益分配部１６に送信する。利益分配部１６は、JASRACに対する請求金額および支払金額を算出し、その情報を出納部２０に送信する。出納部２０は、図示せぬ外部の銀行等と通信し、決算処理を実行する。著作権管理部１３は、ユーザのコンテンツの使用実績をJASRACに送信する。

【００９４】

次に、供給された、暗号化されているコンテンツをメモリスティックに記憶させ、不正の防止を図りつつ、そのコンテンツを他の再生装置などで利用できるようにしたユーザホームネットワーク５の実施の形態の構成を図３０に示す。図１０の場合と同様の部分には、同一の番号を付してあり、その説明は適宜省略する。なお、図３０において、ICカードインターフェース６４およびICカード５５の図示を省略する。

【００９５】

レシーバ５１に装着され、コンテンツを記憶するメモリスティック１１１は、コンテンツ等の記憶等を制御する制御ブロック１２１および実際にコンテンツ等を記憶する情報記憶ブロック１２２からなる。制御ブロック１２１は、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出せない耐タンパー性を有する。

【００９６】

制御ブロック１２１は、通信部１２１、メモリコントローラ１３２、相互認証部１３３、暗号化部１３４、記憶部１３５、復号部１３６、乱数生成部１３７、およびデータ検査部１３８からなる。通信部１３１は、レシーバ５１からコンテンツまたは暗号化されたコンテンツ鍵Ｋｃｏ等を受信し、レシーバ５１にコンテンツまたは暗号化されたコンテンツ鍵Ｋｃｏなどを送信する。メモリコントローラ１３２は、通信部１３１が受信した暗号化されたコンテンツまたはコンテンツ鍵Ｋｃｏ等を、情報記憶ブロック１２２に書き込み、また、情報記憶ブロック１２２に書き込まれたコンテンツ等を読み出し、通信部１３１等に供給する。相互認証部１３３は、レシーバ５１の相互認証モジュール７１と、相互認証処理により、相互認証し、相互認証後、レシーバ５１との通信で、所定の期間利用される一時鍵Ｋｔｅｍｐを生成する。

【００９７】

暗号化部１３４は、一旦、復号部１３６が復号したコンテンツ鍵Ｋｃｏを、保存用鍵Ｋｓａｖｅで暗号化し、メモリコントローラ１３２に供給する。復号部１３６は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏ、または保存用鍵Ｋｓａｖｅで暗号化されたコンテンツ鍵Ｋｃｏなどを復号し、暗号化部１３４または通信部１３１に供給する。記憶部１３５は、そのメモリスティック１１１に固有の（メモリスティック１１１毎に、異なる）値を有する保存用鍵Ｋｓａｖｅおよび検査用鍵Ｋｃｈなどを記憶し、暗号化部１３４または復号部１３６に供給する。記憶部１３５の記憶の態様については、図３６および図３８で詳細に説明する。

【００９８】

乱数生成部１３７は、後述する情報記憶ブロック１２２に記憶されている平文（暗号化されていない）のコンテンツを、メモリスティック１１１内部で暗号化するときに必要な鍵である、所定の桁数の乱数を生成する。データ検査部１３８は、記憶部１３５に記憶されている所定の検査値（検査用のデータ）と後述する鍵データ１４３に記憶されている所定のデータのハッシュ値とを比較することにより、情報記憶ブロック１２２に記憶されている記憶されているコンテンツ鍵Ｋｃｏおよび使用許諾条件情報などが改竄されていないか否かを検査する。データ検査部１３８は、また、情報記憶ブロック１２２に記憶されているコンテンツの移動または情報記憶ブロック１２２へのコンテンツの書き込みのとき、所定の検査値を生成し、記憶部１３５に記憶させる。

【００９９】

情報記憶ブロック１２２は、EEPROM(Electrically Erasable Programmable Read Only Memory)、フラッシュメモリ、強誘電体メモリなどの電気的に記憶内容を書き換えできる、汎用の不揮発性メモリで構成され、データ検索用テーブル１４１、識別情報１４２、鍵データ１４３、暗号化データ１４４、および非暗号化データ１４５が記憶される。データ検索用テーブル１４１には、鍵データ１４３、暗号化データ１４４、および非暗号化データ１４５として記憶されている情報の内容とその記憶位置を表すデータが記憶されている。識別情報１４２には、記憶されている情報の内容が、暗号化されているか否かを示すデータが記憶される。鍵データ１４３としては、暗号化データ１４４に記憶されているコンテンツ毎に、コンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報が記憶されている。鍵データ１４３の記憶の態様については、図３５および図３７で詳細に説明する。暗号化データ１４４としては、暗号化されたコンテンツが記憶されている。非暗号化データ１４５としては、暗号化されていない、コンテンツの使用許諾情報等が記憶される。

【０１００】

図３０のレシーバ５１は、図１０のレシーバ５１に、メモリスティックインターフェース１１２および外部記憶部１３３が追加されている構成を有する。メモ

リスティックインターフェース１１２は、SAM６２からの信号を所定の形式に変更し、レシーバ５１に装着されたメモリスティック１１１に出力し、また、メモリスティック１１１からの信号を所定の形式に変更し、SAM６２に出力する。外部記憶部１１３は、汎用の不揮発性メモリで構成され、SAM６２から供給されたコンテンツ鍵Ｋｃｏなどを記憶し、記憶しているコンテンツ鍵ＫｃｏなどをSAM６２に出力するようになされている。外部記憶部１１３のの記憶の態様については、図３１および図３３で詳細に説明する。

【０１０１】

更に、図３０のSAM６２は、図１０のSAM６２データ検査モジュール１１４を有する。データ検査モジュール１１４は、記憶モジュール７３に記憶されている所定の検査データと外部記憶部１１３が記憶する所定のデータのハッシュ値を比較することにより、外部記憶部１１３に記憶されている記憶されているコンテンツ鍵Ｋｃｏおよび使用許諾条件情報などが改竄されていないか否かを検査する。データ検査モジュール１１４は、また、HDD５２に記憶されているコンテンツの移動またはHDD５２へのコンテンツの書き込みのとき、所定の検査値を生成し、記憶モジュール７３に記憶させる。

【０１０２】

外部記憶部１１３の記憶の態様について、図３１を参照して説明する。外部記憶部１１３の記憶領域は、所定の数の鍵データブロックに分割されている（図３１では、５つの鍵データブロックに分割されている）。それぞれの鍵データブロックは、例えば、２組のコンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報を記憶できる。鍵データブロックに記憶されている１組のコンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報は、コンテンツIDで特定されるHDD５２に記憶されているコンテンツに対応している。鍵データブロック４の前半部分に記憶されていたコンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報に対応するコンテンツが、HDD５２から、メモリスティック１１１に移動したとき、鍵データブロック４の前半部分に記憶されていたコンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報は、消去され、図３１に示すように、鍵データブロック４の前半部分にコンテンツ鍵Ｋｃｏ等が記憶されていない部分が

生じる。同様の操作で、図３１の鍵データブロック３の後半部分もコンテンツ鍵Ｋｃｏ等が記憶されていない。

【０１０３】

図３２は、ユーザホームネットワーク５が、図３０に示す構成を有するときの、記憶モジュール７３の記憶の態様を説明する図である。図３２の記憶モジュール７３は、ユーザの秘密鍵Ｋｓｕ、課金情報、保存用鍵Ｋｓａｖｅ、および配送用鍵Ｋｄに加えて、図３１で説明した、外部記憶部１１３の鍵データブロックに対応する検査値を記憶する。例えば、記憶モジュール７３の検査値１は、データ検査モジュール１１４が、外部記憶部１１３の鍵データブロック１のデータ（すなわち、コンテンツ鍵Ｋｃｏ１、コンテンツID１、使用許諾条件情報１、コンテンツ鍵Ｋｃｏ２、コンテンツID２、および使用許諾条件情報２）にハッシュ関数を適用して得られた値であり、同様に、検査値２は、データ検査モジュール１１４が、鍵データブロック２のデータにハッシュ関数を適用して得られた値である。検査値３、検査値４、および検査値５は、同様に、鍵データブロック３、鍵データブロック４、および鍵データブロック５にそれぞれ対応する。

【０１０４】

すなわち、例えば、鍵データブロック３にハッシュ関数を適用して得られたハッシュ値と検査値３が一致すれば、鍵データブロック３に記憶されているコンテンツ鍵Ｋｃｏ５、コンテンツID５、および使用許諾条件情報５は、改竄されていないことがわかる。一方、鍵データブロック３にハッシュ関数を適用して得られたハッシュ値と検査値３が一致しなければ、鍵データブロック３に記憶されているコンテンツ鍵Ｋｃｏ５、コンテンツID５、および使用許諾条件情報５のいずれかが、改竄されていると判定できる。

【０１０５】

検査値は、耐タンパー性のあるSAM６２の記憶モジュール７３に記憶され、外部から不正に読み出すことが困難であるので、改竄が防止され、従って、図３０に示すレシーバ５１に記憶されたコンテンツ鍵ＫｃｏおよびHDD５２に記憶されたコンテンツは、不正に対して極めて耐性が高い。

【０１０６】

図３３は、外部記憶部１１３の他の記憶の態様を説明する図である。図３３に示す場合、外部記憶部１１３は、コンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報の組に加えて、鍵データブロックに対応した検査値も記憶する。図３３における、例えば、外部記憶部１１３の検査値１は、データ検査モジュール１１４が、外部記憶部１１３の鍵データブロック１のデータ（すなわち、コンテンツ鍵Ｋｃｏ１、コンテンツID１、使用許諾条件情報１、コンテンツ鍵Ｋｃｏ２、コンテンツID２、および使用許諾条件情報２）にハッシュ関数を適用して得られた値を、更に、記憶モジュール７３に記憶する、レシーバ５１特有の値を有する検査用鍵Ｋｃｈで暗号化した値である。検査値２、検査値３、検査値４、および検査値５は、同様に、鍵データブロック２、鍵データブロック３、鍵データブロック４、および鍵データブロック５にそれぞれ対応する。

【０１０７】

図３４は、ユーザホームネットワーク５が、図３０に示す構成を有し、外部記憶部１１３が、図３３に示す記憶の態様を有するときの、記憶モジュール７３の記憶の態様を説明する図である。図３４の記憶モジュール７３は、レシーバ５１（ユーザ）の秘密鍵Ｋｓｕ、課金情報、保存用鍵Ｋｓａｖｅ、および配送用鍵Ｋｄに加えて、検査用鍵Ｋｃｈが記憶されている。

【０１０８】

すなわち、例えば、外部記憶部１１３の鍵データブロック３にハッシュ関数を適用して得られたハッシュ値と、外部記憶部１１３の検査値３を検査用鍵Ｋｄで復号した値が一致すれば、外部記憶部１１３の鍵データブロック３に記憶されているコンテンツ鍵Ｋｃｏ５、コンテンツID５、および使用許諾条件情報５は、改竄されていないことがわかる。一方、外部記憶部１１３の鍵データブロック３にハッシュ関数を適用して得られたハッシュ値と、外部記憶部１１３の検査値３を検査用鍵Ｋｄで復号した値が一致しなければ、外部記憶部１１３の鍵データブロック３に記憶されているコンテンツ鍵Ｋｃｏ５、コンテンツID５、および使用許諾条件情報５のいずれかが、改竄されていると判定できる。

【０１０９】

図３１および図３２に示す場合に比較し、図３３に示す外部記憶部１１３および図３４に示す記憶モジュール７３は、検査値が耐タンパー性を有するメモリに較べ低価格な汎用メモリに記憶されるので、大量のコンテンツに対応する検査値を記憶できるレシーバ５１が、安価に実現できる。

【０１１０】

次に、鍵データ１４３の記憶の態様について、図３５を参照して説明する。鍵データ１４３の記憶領域は、所定の数の鍵データブロックに分割されている（図３５では、４つの鍵データブロックに分割されている）。それぞれの鍵データブロックは、例えば、２組のコンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報を記憶できる。鍵データブロックに記憶されている１組のコンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報は、コンテンツIDで特定される暗号化データ１４４に記憶されているコンテンツに対応している。鍵データブロック３の後半部分に記憶されていたコンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報に対応するコンテンツが、メモリスティック１１１から、HDD５２に移動したとき、鍵データブロック４の後半部分に記憶されていたコンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報は、消去され、図３５に示すように、鍵データブロック４の後半部分にコンテンツ鍵Ｋｃｏ等が記憶されていない部分が生じる。

【０１１１】

図３６は、ユーザホームネットワーク５が、図３０に示す構成を有するときの、記憶部１３５の記憶の態様を説明する図である。記憶部１３５は、ユーザの秘密鍵Ｋｓｕ、課金情報、保存用鍵Ｋｓａｖｅ、および配送用鍵Ｋｄに加えて、図３５で説明した、鍵データ１４３の鍵データブロックに対応する検査値を記憶する。例えば、記憶部１３５の検査値１は、データ検査部１３８が、鍵データ１４３の鍵データブロック１のデータ（すなわち、コンテンツ鍵Ｋｃｏ１、コンテンツID１、使用許諾条件情報１、コンテンツ鍵Ｋｃｏ２、コンテンツID２、および使用許諾条件情報２）にハッシュ関数を適用して得られた値であり、同様に、検査値２は、データ検査部１３８が、鍵データブロック２のデータにハッシュ関数

を適用して得られた値である。検査値３および検査値４は、同様に、鍵データブロック３および鍵データブロック４にそれぞれ対応する。

【０１１２】

すなわち、例えば、鍵データ１４３の鍵データブロック３にハッシュ関数を適用して得られたハッシュ値と記憶部１３５の検査値３が一致すれば、鍵データ１４３の鍵データブロック３に記憶されているコンテンツ鍵Ｋｃｏ５、コンテンツID５、および使用許諾条件情報５は、改竄されていないことがわかる。一方、鍵データブロック３にハッシュ関数を適用して得られたハッシュ値と検査値３が一致しなければ、鍵データブロック３に記憶されているコンテンツ鍵Ｋｃｏ５、コンテンツID５、および使用許諾条件情報５のいずれかが、改竄されていると判定できる。

【０１１３】

レシーバ５１のときと同様に、メモリスティック１１１の検査値は、耐タンパー性のある制御ブロック１２１の記憶部１３５に記憶され、外部から不正に読み出すことが困難であるので、改竄が防止され、従って、図３０に示すメモリスティック１１１に記憶されたコンテンツ鍵Ｋｃｏおよびコンテンツは、不正に対して極めて耐性が高い。

【０１１４】

図３７は、鍵データ１４３の他の記憶の態様を説明する図である。図３７に示す場合、鍵データ１４３は、コンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報の組に加えて、鍵データブロックに対応した検査値も記憶する。図３７における、例えば、鍵データ１４３の検査値１は、データ検査部１３８が、鍵データ１４３の鍵データブロック１のデータ（すなわち、コンテンツ鍵Ｋｃｏ１、コンテンツID１、使用許諾条件情報１、コンテンツ鍵Ｋｃｏ２、コンテンツID２、および使用許諾条件情報２）にハッシュ関数を適用して得られた値を、更に、記憶部１３５に記憶する、メモリスティック１１１特有の値を有する検査用鍵Ｋｃｈ（従って、レシーバ５１の記憶モジュール７３が記憶する検査用鍵Ｋｃｈとは、その値が異なる）で暗号化した値である。検査値２、検査値３、および検査値４は、同様に、鍵データブロック２、鍵データブロック３、および鍵データ

ブロック４にそれぞれ対応する。

【０１１５】

図３８は、ユーザホームネットワーク５が、図３０に示す構成を有し、メモリスティック１１１の鍵データ１４３が、図３７に示す記憶の態様を有するときの、記憶部１３５の記憶の態様を説明する図である。図３８の記憶部１３５は、メモリスティック１１１の秘密鍵Ｋｓｕ２、および保存用鍵Ｋｓａｖｅに加えて、検査用鍵Ｋｃｈが記憶されている。

【０１１６】

すなわち、例えば、鍵データ１４３の鍵データブロック３にハッシュ関数を適用して得られたハッシュ値と、鍵データ１４３の検査値３を検査用鍵Ｋｄで復号した値が一致すれば、鍵データ１４３の鍵データブロック３に記憶されているコンテンツ鍵Ｋｃｏ５、コンテンツID５、および使用許諾条件情報５は、改竄されていないことがわかる。一方、鍵データ１４３の鍵データブロック３にハッシュ関数を適用して得られたハッシュ値と鍵データ１４３の検査値３を検査用鍵Ｋｄで復号した値が一致しなければ、鍵データ１４３の鍵データブロック３に記憶されているコンテンツ鍵Ｋｃｏ５、コンテンツID５、および使用許諾条件情報５のいずれかが、改竄されていると判定できる。

【０１１７】

図３７に示す鍵データ１４３および図３８に示す記憶部１３５は、検査値が耐タンパー性を有するメモリに較べ低価格な汎用メモリに記憶されるので、大量のコンテンツに対応する検査値を記憶できるスティックメモリ１１１が、安価に実現できる。

【０１１８】

次に、EMDシステムの処理について説明する。図３９は、このシステムのコンテンツの配布および再生の処理を説明するフローチャートである。ステップＳ１１において、EMDサービスセンタ１のコンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信し、コンテンツプロバイダ２がこれを受信する。その処理の詳細は、図４１のフローチャートを参照して後述する。ステップＳ１２において、ユーザは、ユーザホームネットワーク５の機器（例えば

、図１０のレシーバ５１）を操作し、ユーザホームネットワーク５の機器をEMDサービスセンタ１のユーザ管理部１８に登録する。この登録処理の詳細は、図４５のフローチャートを参照して後述する。ステップＳ１３において、EMDサービスセンタ１のユーザ管理部１８は、ユーザホームネットワーク５と、図４２乃至図４４に示したように相互認証した後、ユーザホームネットワーク５の機器に、配送用鍵Ｋｄを送信する。ユーザホームネットワーク５はこの鍵を受信する。この処理の詳細は、図５３のフローチャートを参照して説明する。

【０１１９】

ステップＳ１４において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、サービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図５５のフローチャートを参照して後述する。ステップＳ１５において、サービスプロバイダ３のセキュアコンテナ作成部４４は、ユーザホームネットワーク５からの要求に応じて、ネットワーク４を介して、ユーザホームネットワーク５にサービスプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図５７のフローチャートを参照して後述する。ステップＳ１６において、ユーザホームネットワーク５の課金モジュール７２は、課金処理を実行する。課金処理の詳細は、図５９のフローチャートを参照して後述する。ステップＳ１７において、ユーザは、ユーザホームネットワーク５の機器でコンテンツを再生する。再生処理の詳細は、図６３のフローチャートを参照して後述する。

【０１２０】

一方、コンテンツプロバイダ２が、取扱方針を暗号化して送信する場合の処理は、図４０のフローチャートで示すようになる。ステップＳ２１において、EMDサービスセンタ１のコンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信する。ステップＳ２２において、EMDサービスセンタ１のサービスプロバイダ管理部１１は、サービスプロバイダ３に配送用鍵Ｋｄを送信する。それ以降のステップＳ２３乃至ステップＳ２８の処理は、図３９のステップＳ１２乃至ステップＳ１７の処理と同様の処理であり、その説明は省略する。

【０１２１】

図４１は、図３９のステップＳ１１および図４０のステップＳ２１に対応する、EMDサービスセンタ１がコンテンツプロバイダ２へ配送用鍵Ｋｄを送信し、コンテンツプロバイダ２がこれを受信する処理の詳細を説明するフローチャートである。ステップＳ３１において、EMDサービスセンタ１の相互認証部１７は、コンテンツプロバイダ２の相互認証部３９と相互認証する。この相互認証処理の詳細は、図４２を参照して後述する。相互認証処理により、コンテンツプロバイダ２が、正当なプロバイダであることが確認されたとき、ステップＳ３２において、コンテンツプロバイダ２の暗号化部３４および暗号化部３６は、EMDサービスセンタ１のコンテンツプロバイダ管理部１２から送信された配送用鍵Ｋｄを受信する。ステップＳ３３において、コンテンツプロバイダ２の暗号化部３４は、受信した配送用鍵Ｋｄを記憶する。

【０１２２】

このように、コンテンツプロバイダ２は、EMDサービスセンタ１から配送用鍵Ｋｄを受け取る。同様に、図４０に示すフローチャートの処理を行う例の場合、コンテンツプロバイダ２以外に、サービスプロバイダ３も、図４１と同様の処理で、EMDサービスセンタ１から配送用鍵Ｋｄを受け取る。

【０１２３】

次に、図４１のステップＳ３１における、いわゆるなりすましがないことを確認する相互認証の処理について、１つの共通鍵を用いる（図４２）、２つの共通鍵を用いる（図４３）、および公開鍵暗号を用いる（図４４）を例として説明する。

【０１２４】

図４２は、１つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ４１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する（乱数生成部３５が生成するようにしてもよい）。ステップＳ４２において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて乱数Ｒ１を、予め記憶している

共通鍵Ｋcで暗号化する（暗号化部３６で暗号化するようにしてもよい）。ステップＳ４３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をEMDサービスセンタ１の相互認証部１７に送信する。

【０１２５】

ステップＳ４４において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋcで復号する。ステップＳ４５において、EMDサービスセンタ１の相互認証部１７は、３２ビットの乱数Ｒ２を生成する。ステップＳ４６において、EMDサービスセンタ１の相互認証部１７は、復号した６４ビットの乱数Ｒ１の下位３２ビットを乱数Ｒ２で入れ替え、連接$R1_H \| R2$を生成する。なお、ここでRi_Hは、Ｒｉの上位ビットを表し、Ａ‖Ｂは、ＡとＢの連接（ｎビットのＡの下位に、ｍビットのＢを結合して、（ｎ＋ｍ）ビットとしたもの）を表す。ステップＳ４７において、EMDサービスセンタ１の相互認証部１７は、DESを用いて$R1_H \| R2$を共通鍵Ｋcで暗号化する。ステップＳ４８において、EMDサービスセンタ１の相互認証部１７は、暗号化した$R1_H \| R2$をコンテンツプロバイダ２に送信する。

【０１２６】

ステップＳ４９において、コンテンツプロバイダ２の相互認証部３９は、受信した$R1_H \| R2$を共通鍵Ｋcで復号する。ステップＳ５０において、コンテンツプロバイダ２の相互認証部３９は、復号した$R1_H \| R2$の上位３２ビット$R1_H$を調べ、ステップＳ４１で生成した、乱数Ｒ１の上位３２ビット$R1_H$と一致すれば、EMDサービスセンタ１が正当なセンタであることを認証する。生成した乱数$R1_H$と、受信した$R1_H$が一致しないとき、処理は終了される。両者が一致するとき、ステップＳ５１において、コンテンツプロバイダ２の相互認証部３９は、３２ビットの乱数Ｒ３を生成する。ステップＳ５２において、コンテンツプロバイダ２の相互認証部３９は、受信し、復号した３２ビットの乱数Ｒ２を上位に設定し、生成した乱数Ｒ３をその下位に設定し、連接Ｒ２‖Ｒ３とする。ステップＳ５３において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて連接Ｒ２‖Ｒ３を共通鍵Ｋcで暗号化する。ステップＳ５４において、コンテンツプロバイダ２の相互認証部３９は、暗号化された連接Ｒ２‖Ｒ３をEMDサービ

スセンタ１の相互認証部１７に送信する。

【０１２７】

ステップＳ５５において、EMDサービスセンタ１の相互認証部１７は、受信した連接Ｒ２‖Ｒ３を共通鍵Kcで復号する。ステップＳ５６において、EMDサービスセンタ１の相互認証部１７は、復号した連接Ｒ２‖Ｒ３の上位３２ビットを調べ、乱数Ｒ２と一致すれば、コンテンツプロバイダ２を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

【０１２８】

図４３は、２つの共通鍵Ｋｃ１，Ｋｃ２で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ６１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ６２において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で暗号化する。ステップＳ６３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をEMDサービスセンタ１に送信する。

【０１２９】

ステップＳ６４において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で復号する。ステップＳ６５において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ１を予め記憶している共通鍵Ｋｃ２で暗号化する。ステップＳ６６において、EMDサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ６７において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ２を共通鍵Ｋｃ２で暗号化する。ステップＳ６８において、EMDサービスセンタ１の相互認証部１７は、暗号化された乱数Ｒ１および乱数Ｒ２をコンテンツプロバイダ２の相互認証部３９に送信する。

【０１３０】

ステップＳ６９において、コンテンツプロバイダ２の相互認証部３９は、受信した乱数Ｒ１および乱数Ｒ２を予め記憶している共通鍵Ｋｃ２で復号する。ステ

ップＳ７０において、コンテンツプロバイダ２の相互認証部３９は、復号した乱数Ｒ１を調べ、ステップＳ６１で生成した乱数Ｒ１（暗号化する前の乱数Ｒ１）と一致すれば、EMDサービスセンタ１を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップＳ７１において、コンテンツプロバイダ２の相互認証部３９は、復号して得た乱数Ｒ２を共通鍵Ｋｃ１で暗号化する。ステップＳ７２において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ２をEMDサービスセンタ１に送信する。

【０１３１】

ステップＳ７３において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ２を共通鍵Ｋｃ１で復号する。ステップＳ７４において、EMDサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ６６で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

【０１３２】

図４４は、公開鍵暗号である、１６０ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ８１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ８２において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐを含む証明書（認証局から予め取得しておいたもの）と、乱数Ｒ１をEMDサービスセンタ１の相互認証部１７に送信する。

【０１３３】

ステップＳ８３において、EMDサービスセンタ１の相互認証部１７は、受信した証明書の署名（認証局の秘密鍵Ｋｓｃａで暗号化されている）を、予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、コンテンツプロバイダ２の公開鍵Ｋｐｃｐとコンテンツプロバイダ２の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前を取り出す。証明書が認証局が発行した適正なも

のであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵Ｋｐｃｐが改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

【０１３４】

適正な認証結果が得られたとき、ステップＳ８４において、EMDサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ８５において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ１および乱数Ｒ２の連接Ｒ１‖Ｒ２を生成する。ステップＳ８６において、EMDサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を自分自身の秘密鍵Ｋｓｅｓｃで暗号化する。ステップＳ８７において、EMDサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を、ステップＳ８３で取得したコンテンツプロバイダ２の公開鍵Ｋｐｃｐで暗号化する。ステップＳ８８において、EMDサービスセンタ１の相互認証部１７は、秘密鍵Ｋｓｅｓｃで暗号化された連接Ｒ１‖Ｒ２、公開鍵Ｋｐｃｐで暗号化された連接Ｒ１‖Ｒ２、および自分自身の公開鍵Ｋｐｅｓｃを含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ２の相互認証部３９に送信する。

【０１３５】

ステップＳ８９において、コンテンツプロバイダ２の相互認証部３９は、受信した証明書の署名を予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、正しければ証明書から公開鍵Ｋｐｅｓｃを取り出す。この場合の処理は、ステップＳ８３における場合と同様であるので、その説明は省略する。ステップＳ９０において、コンテンツプロバイダ２の相互認証部３９は、EMDサービスセンタ１の秘密鍵Ｋｓｅｓｃで暗号化されている連接Ｒ１‖Ｒ２を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで復号する。ステップＳ９１において、コンテンツプロバイ

ダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐで暗号化されている連接Ｒ１‖Ｒ２を、自分自身の秘密鍵Ｋｓｃｐで復号する。ステップＳ９２において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で復号された連接Ｒ１‖Ｒ２と、ステップＳ９１で復号された連接Ｒ１‖Ｒ２を比較し、一致すればEMDサービスセンタ１を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【０１３６】

適正な認証結果が得られたとき、ステップＳ９３において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ３を生成する。ステップＳ９４において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で取得した乱数Ｒ２および生成した乱数Ｒ３の連接Ｒ２‖Ｒ３を生成する。ステップＳ９５において、コンテンツプロバイダ２の相互認証部３９は、連接Ｒ２‖Ｒ３を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで暗号化する。ステップＳ９６において、コンテンツプロバイダ２の相互認証部３９は、暗号化した連接Ｒ２‖Ｒ３をEMDサービスセンタ１の相互認証部１７に送信する。

【０１３７】

ステップＳ９７において、EMDサービスセンタ１の相互認証部１７は、暗号化された連接Ｒ２‖Ｒ３を自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ９８において、EMDサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ８４で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなけば、不適正なプロバイダとして、処理を終了する。

【０１３８】

以上のように、EMDサービスセンタ１の相互認証部１７とコンテンツプロバイダ２の相互認証部３９は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵Ｋｔｅｍｐとして利用される。

【０１３９】

図４５は、図３９のステップＳ１２および図４０のステップＳ２３に対応する、レシーバ５１がEMDサービスセンタ１のユーザ管理部１８に登録する処理を説

明するフローチャートである。ステップＳ１０１において、レシーバ５１のSAM６２は、ICカードインターフェース６４の出力から、レシーバ５１にバックアップ用のICカード５５が装着されているか否かを判定し、バックアップ用のICカード５５が装着されていると判定された場合（例えば、レシーバ５１が新たなレシーバ５１に変更され、元のレシーバ５１のデータを、新たなレシーバ５１に引き継ぐために、元のレシーバ５１のデータをバックアップ用のICカード５５にバックアップさせている場合）、ステップＳ１０２に進み、ICカード５５に記憶されているバックアップデータの読み込み処理を実行する。この処理の詳細は、図５０のフローチャートを参照して後述する。勿論、この読み込み処理が実行されるためには、その前に、ICカード５５に、バックアップデータを記憶させる必要があるが、その処理は、図４８を参照して後述する。

【０１４０】

ステップＳ１０１において、バックアップ用のICカード５５が装着されていないと判定された場合、手続は、ステップＳ１０２をスキップし、ステップＳ１０３に進む。ステップＳ１０３において、SAM６２の相互認証モジュール７１は、EMDサービスセンタ１の相互認証部１７と相互認証し、SAM６２は、証明書をEMDサービスセンタ１のユーザ管理部１８に送信する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１０３で、SAM６２がEMDサービスセンタ１のユーザ管理部１８に送信する署名書は、図４６に示すデータを含む。SAM６２が送信する証明書は、図１４に示すコンテンツプロバイダ２の証明書とほぼ同様の構成を有するが、更に、他のSAMに従属するか否かを示すデータを含んでいる。ステップＳ１０４において、SAM６２は、通信部６１を介して、一時鍵Ｋｔｅｍｐで暗号化した、ユーザの銀行等の決済機関の情報等をEMDサービスセンタ１のユーザ管理部１８に送信する。

【０１４１】

ステップＳ１０５において、EMDサービスセンタ１のユーザ管理部１８は、受信したSAM６２のIDを基に、図７に示したユーザ登録データベースを検索する。ステップＳ１０６において、EMDサービスセンタ１のユーザ管理部１８は、受信したIDを有するSAM６２の登録が可能であるか否かを判定し、受信したIDを有す

るSAM６２の登録が可能であると判定された場合、ステップＳ１０７に進み、受信したIDを有するSAM６２が、新規登録であるか否かを判定する。ステップＳ１０７において、受信したIDを有するSAM６２が、新規登録ではないと判定された場合、手続は、ステップＳ１０８に進む。

【０１４２】

ステップＳ１０８において、EMDサービスセンタ１のユーザ管理部１８は、更新登録を実行し、受信したIDを基にユーザ登録データベースを検索し、登録リストを作成する。この登録リストは、例えば、図４７に示す構造を有し、機器のSAMのIDに対応して、EMDサービスセンタ１のユーザ管理部１８が登録を拒絶したか否かを示す登録拒絶フラグ、従属する機器である場合のコンテンツ鍵Ｋｃｏの利用条件を示すステータスフラグ、従属する機器であるか否かを示すコンディションフラグ、並びに登録拒絶フラグ、ステータスフラグ、およびコンディションフラグにハッシュ関数を適用して生成したハッシュ値をEMDサービスセンタ１の秘密鍵Ｋｓｅｓｃで暗号化した署名から構成される。

【０１４３】

機器のSAMのIDは、機器の固有の６４ビットからなるIDを示す（図４７では、１６進数で示す）。登録拒絶フラグの”１”は、EMDサービスセンタ１のユーザ管理部１８が対応するIDを有する機器を登録したことを示し、登録拒絶フラグの”０”は、MDサービスセンタ１のユーザ管理部１８が対応するIDを有する機器の登録を拒絶したことを示す。

【０１４４】

ステータスフラグのMSB(Most Significant Bit)の”１”は、対応するIDを有する子の機器（例えばレコーダ５３）が従属した親の機器（例えばレシーバ５１）からコンテンツ鍵Ｋｃｏをもらえることを示し、ステータスフラグのMSBの”０”は、対応するIDを有する子の機器が従属した親の機器からコンテンツ鍵Ｋｃｏをもらえないことを示している。ステータスフラグの上位から２ビット目の”１”は、対応するIDを有する子の機器が従属した親の機器から、親の機器の保存用鍵Ｋｓａｖｅで暗号化されたコンテンツ鍵Ｋｃｏをもらえることを示す。ステータスフラグの上位から３ビット目の”１”は、対応するIDを有する子の機器が

従属した親の機器から、配送用鍵Ｋｄで暗号化されたコンテンツ鍵Ｋｃｏをもらえることを示す。ステータスフラグのLSB(Least Significant Bit)の”１”は、従属した親の機器が配送用鍵Ｋｄで暗号化したコンテンツ鍵Ｋｃｏを購入し、対応するIDを有する子の機器に、一時鍵Ｋｔｅｍｐで暗号化してコンテンツ鍵Ｋｃｏを渡すことを示す。

【０１４５】

コンディションフラグの”０”は、対応するIDを有する機器がEMDサービスセンタ１のユーザ管理部１８と直接通信が出来る（すなわち、例えばレシーバ５１のような親の機器である）ことを示し、コンディションフラグの”１”は、対応するIDを有する機器がEMDサービスセンタ１のユーザ管理部１８と直接通信が出来ない（すなわち、例えばレコーダ５３のような子の機器である）ことを示す。コンディションフラグが”０”のとき、ステータスフラグは常に”００００”に設定される。

【０１４６】

ステップＳ１０９において、EMDサービスセンタ１のユーザ管理部１８は、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで暗号化した、鍵サーバ１４から供給された配送用鍵Ｋｄをレシーバ５１のSAM６２に送信する。ステップＳ１１０において、レシーバ５１のSAM６２は、受信した配送用鍵Ｋｄを一時鍵Ｋｔｅｍｐで復号し、記憶モジュール７３に記憶させる。

【０１４７】

ステップＳ１１１において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化した登録リストをレシーバ５１のSAM６２に送信する。ステップＳ１１２において、レシーバ５１のSAM６２は、受信した登録リストを一時鍵Ｋｔｅｍｐで復号し、記憶モジュール７３に記憶させ、処理は終了する。

【０１４８】

ステップＳ１０７において、受信したIDを有するSAM６２が、新規登録であると判定された場合、手続は、ステップＳ１１４に進み、EMDサービスセンタ１のユーザ管理部１８は、新規登録を実行し、登録リストを作成し、ステップＳ１０９に進む。

【０１４９】

ステップＳ１０６において、受信したIDを有するSAM６２の登録が不可であると判定された場合、ステップＳ１１３に進み、EMDサービスセンタ１のユーザ管理部１８は、登録拒絶の登録リストを作成し、ステップＳ１１１に進む。

【０１５０】

このように、レシーバ５１は、EMDサービスセンタ１に登録される。

【０１５１】

次に、今まで使用していたレシーバ５１の記憶モジュール７３に記憶された配送用鍵Ｋｄなどの所定のデータをICカード５５に記憶させる処理の詳細を、図４８のフローチャートを参照して説明する。ステップＳ１２１において、SAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１２２において、SAM６２の乱数発生ユニット９２は、バックアップ鍵Ｋｉｃとして用いられる乱数を生成する。ステップＳ１２３において、SAM６２の暗号化ユニット９３は、記憶モジュール７３に記憶されているSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを、バックアップ鍵Ｋｉｃを用いて暗号化する。ステップＳ１２４において、SAM６２の暗号化ユニット９３は、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃでバックアップ鍵Ｋｉｃを暗号化する（SAM６２は、EMDサービスセンタ１との間の認証処理（図４４のステップＳ８９）において、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを取得している）。ステップＳ１２５において、レシーバ５１のSAM６２は、ICカードインターフェース６４を介して、暗号化されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のID並びに暗号化されたバックアップ鍵ＫｉｃをICカード５５に送信し、記憶モジュール８１に記憶させる。

【０１５２】

以上のように、SAM６２の記憶モジュール７３に記憶されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDは、バックアップ鍵Ｋｉｃを用いて暗号化され、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを用いて暗号化されたバックアップ鍵Ｋｉｃと共に、ICカード５５の記憶モジュール８１に記憶される。

【０１５３】

今まで使用していたレシーバ５１の記憶モジュール７３に記憶された配送用鍵Ｋｄなどの所定のデータをICカード５５に記憶させる他の処理の例の詳細を、図４９のフローチャートを参照して説明する。ステップＳ１３１において、SAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。ステップＳ１３２において、SAM６２の暗号化ユニット９３は、記憶モジュール７３に記憶されているSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを用いて暗号化する。ステップＳ１３３において、レシーバ５１のSAM６２は、ICカードインターフェース６４を介して、暗号化されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDをICカード５５に送信し、記憶モジュール８１に記憶させる。

【０１５４】

図４９に示す処理により、図４８に示した場合より簡単な処理で、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃを用いて暗号化されたSAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDは、ICカード５５の記憶モジュール８１に記憶される。

【０１５５】

このように、ICカード５５にバックアップされたデータは、図４５のステップＳ１０２の処理で、新しいレシーバ５１に読み込まれる。図５０は、図４８に示す処理でバックアップされたデータ読み出す場合の処理を説明するフローチャートである。ステップＳ１４１において、新しいレシーバ５１のSAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０１５６】

ステップＳ１４２において、SAM６２は、ICカードインタフェース６４を介して、記憶モジュール８１に記憶された、バックアップ鍵Ｋｉｃで暗号化されている古いレシーバ５１の記憶モジュール７３のデータ（SAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを示すバックアップデータ）、およびEMDサービス

センタ１の公開鍵Ｋｐｅｓｃで暗号化されているバックアップ鍵Ｋｉｃを読み出す。ステップＳ１４３において、SAM６２の相互認証モジュール７１は、通信部６１を介して、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１４４において、SAM６２は、通信部６１を介して、バックアップ鍵Ｋｉｃで暗号化されている記憶モジュール７３のデータ、およびEMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されているバックアップ鍵Ｋｉｃを、EMDサービスセンタ１のユーザ管理部１８に送信する。

【０１５７】

ステップＳ１４５において、EMDサービスセンタ１のユーザ管理部１８は、受信したバックアップ鍵Ｋｉｃを自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ１４６において、EMDサービスセンタ１のユーザ管理部１８は、受信したバックアップデータを、バックアップ鍵Ｋｉｃで復号する。ステップＳ１４７において、EMDサービスセンタ１のユーザ管理部１８は、復号したバックアップデータを、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで、再度、暗号化する。ステップＳ１４８において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化されたバックアップデータを、レシーバ５１の通信部６１に送信する。

【０１５８】

ステップＳ１４９において、レシーバ５１の通信部６１は、EMDサービスセンタ１のユーザ管理部１８から受信したデータを、SAM６２に送信し、SAM６２は、そのデータを復号した後、記憶モジュール７３に記憶させる。ステップＳ１６０において、EMDサービスセンタ１のユーザ管理部１８は、ICカード５５にデータを記憶させた古い装置のSAM６２のIDに対応するユーザ登録データベース（図７）のデータを登録不可に設定し、処理を終了する。

【０１５９】

このように、新しいレシーバ５１は、ICカード５５のバックアップデータを読み込む。

【０１６０】

図４９に示す処理でバックアップされたデータ読み出す場合の処理を、図５１に示すフローチャートを用いて説明する。ステップＳ１６１において、新しいレシーバ５１のSAM６２の相互認証モジュール７１は、ICカード５５の相互認証モジュール８０と相互認証する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１６２において、SAM６２は、ICカードインタフェース６４を介して、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されている古いレシーバ５１の記憶モジュール７３のデータ（SAMのID番号、保存用鍵Ｋｓａｖｅ、およびHDD５２のIDを示すバックアップデータ）を読み出す。

【０１６１】

ステップＳ１６３において、SAM６２の相互認証モジュール７１は、通信部６１を介して、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１６４において、SAM６２は、通信部６１を介して、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃで暗号化されている記憶モジュール７３のデータを、EMDサービスセンタ１のユーザ管理部１８に送信する。

【０１６２】

ステップＳ１６５において、EMDサービスセンタ１のユーザ管理部１８は、受信した記憶モジュール７３のデータを自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ１６６において、EMDサービスセンタ１のユーザ管理部１８は、復号したバックアップデータを、相互認証部１７から供給された一時鍵Ｋｔｅｍｐで、再度、暗号化する。ステップＳ１６７において、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｔｅｍｐで暗号化されたバックアップデータを、レシーバ５１の通信部６１に送信する。

【０１６３】

ステップＳ１６８において、レシーバ５１の通信部６１は、EMDサービスセンタ１のユーザ管理部１８から受信したデータを、SAM６２に送信し、SAM６２は、そにのデータを復号した後、記憶モジュール７３に記憶させる。ステップＳ１６

９において、EMDサービスセンタ１のユーザ管理部１８は、ICカード５５にデータを記憶させた古い装置のSAM６２のIDに対応するユーザ登録データベース（図７）のデータを登録不可に設定する。

【０１６４】

このように、図４９に示す処理を用いたバックアップの場合、図５１に示す処理により、新しいレシーバ５１は、ICカード５５のバックアップデータを読み込む。

【０１６５】

レシーバ５１は、自分自身を登録する場合（図３９のステップＳ１２に対応する処理を実行する場合）、図４５のフローチャートに示す処理を実行するが、レシーバ５１に従属するレコーダ５３をEMDサービスセンタ１に登録する場合、図５２のフローチャートに示す処理を実行する。ステップＳ１８１において、レシーバ５１のSAM６２は、記憶モジュール７３に記憶された登録リストに、レコーダ５３のIDを書き込む。ステップＳ１８２において、レシーバ５１の相互認証モジュール７１は、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０１６６】

ステップＳ１８３において、EMDサービスセンタ１のユーザ管理部１８は、レシーバ５１のID（図４６に示すSAM６２の証明書に含まれるSAM６２のID）を基に、ユーザ登録データベースを検索し、レシーバ５１が登録不可であるか否かを判定し、レシーバ５１が登録不可ではないと判定された場合、ステップＳ１８４に進み、レシーバ５１のSAM62は、EMDサービスセンタ１のユーザ管理部１８に、記憶モジュール７３に記憶している配送用鍵Ｋｄのバージョン、課金情報（後述の図５９に示すフローチャートのステップＳ３３７の処理で記憶される）、および登録リスト、並びにHDD５２に記録された取扱方針を一時鍵Ｋｔで暗号化し、通信部６１を介して、EMDサービスセンタ１のユーザ管理部１８に、記憶モジュール７３に記憶している配送用鍵Ｋｄのバージョン、課金情報、および登録リスト、並びにHDD５２に記録された取扱方針を送信する。ステップＳ１８５において

、EMDサービスセンタ１のユーザ管理部１８は、受信したデータを復号した後、課金情報を処理し、図４７を参照して説明した、レシーバ５１から受信した登録リストのレコーダ５３に関する登録拒絶フラグ、およびステータスフラグなどのデータの部分を更新し、レシーバ５１に対応するデータに応じた署名を付する。

【０１６７】

ステップＳ１８６において、EMDサービスセンタ１のユーザ管理部１８は、レシーバ５１が有する配送用鍵Ｋｄのバージョンが最新か否かを判定し、レシーバ５１が有する配送用鍵Ｋｄのバージョンが最新であると判定された場合、ステップＳ１８７に進み、一時鍵Ｋｄで暗号化した、更新した登録リスト、および課金情報受信メッセージを、レシーバ５１に送信し、レシーバ５１は、更新した登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップＳ１８８において、レシーバ５１は、記憶モジュール７３に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ１のユーザ管理部１８からステップＳ１８７において受信したものに更新し、ステップＳ１９１に進む。

【０１６８】

ステップＳ１８６において、レシーバ５１が有する配送用鍵Ｋｄのバージョンが最新のものではないと判定された場合、ステップＳ１８９に進み、EMDサービスセンタ１のユーザ管理部１８は、一時鍵Ｋｄで暗号化した、最新バージョンの配送用鍵Ｋｄ、更新した登録リスト、および課金情報受信メッセージを、レシーバ５１に送信し、レシーバ５１は、最新バージョンの配送用鍵Ｋｄ、更新した登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップＳ１９０において、レシーバ５１は、記憶モジュール７３に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ１のユーザ管理部１８からステップＳ１８９において受信したものに更新し、配送用鍵Ｋｄを最新バージョンのものに更新し、ステップＳ１９１に進む。

【０１６９】

ステップＳ１９１において、レシーバ５１のSAM６２は、更新した登録リストを参照し、レコーダ５３が登録不可か否かを判定し、レコーダ５３が登録不可でないと判定された場合、ステップＳ１９２に進み、レシーバ５１とレコーダ５３

は相互認証し、一時鍵Ｋｔｅｍｐを共有する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ１９３において、レコーダ５３に、一時鍵Ｋｄで暗号化した、登録完了メッセージ、および配送用鍵Ｋｄを送信し、レコーダ５３は、登録完了メッセージ、および配送用鍵Ｋｄを受信し、復号する。ステップＳ１９４において、レコーダ５３は、配送用鍵Ｋｄを更新し、処理は終了する。

【０１７０】

ステップＳ１８３において、レシーバ５１が登録不可であると判定された場合、および、ステップＳ１９１において、レコーダ５３が登録不可であると判定された場合、処理は終了する。

【０１７１】

以上のように、レシーバ５１に従属するレコーダ５３は、レシーバ５１を介して、EMDサービスセンタ１に登録される。

【０１７２】

図５３は、図３９のステップＳ１３において、EMDサービスセンタ１がレシーバ５１に送信した配送用鍵Ｋｄを、レシーバ５１が受け取る処理の詳細を説明するフローチャートである。ステップＳ２０１において、レシーバ５１の相互認証モジュール７１は、EMDサービスセンタ１の相互認証部１７と相互認証する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２０２において、レシーバ５１のSAM６２は、通信部６１を介して、EMDサービスセンタ１のユーザ管理部１８に証明書を送信し、EMDサービスセンタ１のユーザ管理部１８は、証明書を受信する。ステップＳ２０３乃至ステップＳ２１０は、図５２のステップＳ１８３乃至ステップＳ１９０と同様の処理であるのでその説明は省略する。

【０１７３】

このように、レシーバ５１は、EMDサービスセンタ１のユーザ管理部１８から配送用鍵Ｋｄを受け取り、レシーバ５１の課金情報をEMDサービスセンタ１のユーザ管理部１８に送信する。

【０１７４】

次に、ユーザネットワーク５が図１０または図１１の構成を有する場合、レシーバ５１に従属するレコーダ５３の配送用鍵Ｋｄの受け取り処理（図４７に示すステータスフラグが、レコーダ５３の配送用鍵Ｋｄの受け取りを許可する値を有する場合）を、図５４に示すフローチャートを用いて説明する。ステップＳ２２１において、レシーバ５１の相互認証モジュール７１およびレコーダ５３の図示せぬ相互認証モジュールは、相互認証する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０１７５】

ステップＳ２２２において、レシーバ５１は、レシーバ５１の記憶モジュール７３に記憶する登録リストにレコーダ５３のデータが載っているか否かを判定し、レシーバ５１の記憶モジュール７３に記憶する登録リストにレコーダ５３のデータが載っていると判定された場合、ステップＳ２２３に進み、レシーバ５１の記憶モジュール７３に記憶する登録リストを基に、レコーダ５３が登録不可であるか否かを判定する。ステップＳ２２３において、レコーダ５３が登録不可ではないと判定された場合、ステップＳ２２４に進み、レコーダ５３のSAM６６は、レシーバ５１のSAM６２に、内蔵する記憶モジュールに記憶している配送用鍵Ｋｄ（後述する図５４のステップＳ２３５でレシーバ５１から受け取っている）のバージョンおよび課金情報（後述する図５９に対応する処理のステップＳ３３７に相当する処理で記憶している）を一時鍵Ｋｔｅｍｐで暗号化して、送信し、レシーバ５１のSAM６２は、配送用鍵Ｋｄのバージョンおよび課金情報を受信し、復号する。

【０１７６】

ステップＳ２２５において、レシーバ５１の相互認証モジュール７１は、通信部６１を介して、EMDサービスセンタ１の相互認証部１７と、相互認証する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２２６において、EMDサービスセンタ１のユーザ管理部１８は、レシーバ５１のIDを基に、ユーザ登録データベースを検索し、レシーバ５１が登録不可であるか否かを判定し、レシーバ５１が登録不可では

ないと判定された場合、ステップＳ２２７に進み、レシーバ５１のSAM62は、通信部６１を介して、EMDサービスセンタ１のユーザ管理部１８に、一時鍵Ｋｄで暗号化した、記憶モジュール７３に記憶している配送用鍵Ｋｄのバージョン、課金情報、および登録リスト、HDD５２に記録している取扱方針、並びにレコーダ５３の課金情報を送信する。ステップＳ２２８において、EMDサービスセンタ１のユーザ管理部１８は、受信したデータを復号した後、課金情報を処理し、図４７で説明した、レシーバ５１から受信した登録リストのレコーダ５３に関する登録拒絶フラグ、ステータスフラグなどのデータの部分を更新し、レシーバ５１に対応するデータに応じた署名を付する。

【０１７７】

ステップＳ２２９乃至ステップＳ２３４の処理は、図５２に示すステップＳ１８６乃至ステップＳ１９１とそれぞれ同様であるので、その説明は省略する。

【０１７８】

ステップＳ２３４において、レシーバ５１のSAM６２は、更新した登録リストを参照し、レコーダ５３が登録不可か否かを判定し、レコーダ５３が登録不可でないと判定された場合、ステップＳ２３５に進み、レコーダ５３に、一時鍵Ｋｄで暗号化した、課金情報受信メッセージ、および配送用鍵Ｋｄを送信し、レコーダ５３は、課金情報受信メッセージ、および配送用鍵Ｋｄを受信し、復号する。ステップＳ２３６において、レコーダ５３のSAM６６は、内蔵する記憶モジュールに記憶している、課金情報を消去し、配送用鍵Ｋｄを最新のバージョンに更新する。

【０１７９】

ステップＳ２２２において、レシーバ５１の記憶モジュール７３に記憶する登録リストにレコーダ５３のデータが載っていないと判定された場合、ステップＳ２３７に進み、図５２に示したレコーダ５３の登録処理を実行し、ステップＳ２２４に進む。

【０１８０】

ステップＳ２２３において、レコーダ５３が登録不可であると判定された場合、ステップＳ２２６において、レシーバ５１が登録不可であると判定された場合

、および、ステップＳ２３４において、レコーダ５３が登録不可であると判定された場合、処理は終了する。

【０１８１】

以上のように、レシーバ５１に従属するレコーダ５３は、レシーバ５１を介して、配送用鍵Ｋｄを受け取る。

【０１８２】

次に、図３９のステップＳ１４に対応する、コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する処理を、図５５のフローチャートを用いて説明する。ステップＳ２５１において、コンテンツプロバイダ２のウォータマーク付加部３２は、コンテンツサーバ３１から読み出したコンテンツに、コンテンツプロバイダ２を示す所定のウォータマークを挿入し、圧縮部３３に供給する。ステップＳ２５２において、コンテンツプロバイダ２の圧縮部３３は、ウォータマークが挿入されたコンテンツをATRAC2等の所定の方式で圧縮し、暗号化部３４に供給する。ステップＳ２５３において、乱数発生部３５は、コンテンツ鍵Ｋｃｏとして用いる乱数を発生させ、暗号化部３４に供給する。ステップＳ２５４において、コンテンツプロバイダ２の暗号化部３４は、DESなどの所定の方式で、コンテンツ鍵Ｋｃｏを使用して、ウォータマークが挿入され、圧縮されたコンテンツを暗号化する。

【０１８３】

ステップＳ２５５において、暗号化部３６は、DESなどの所定の方式で、図３９のステップＳ１１の処理により、EMDサービスセンタ１から供給されている配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを暗号化する。ステップＳ２５６において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、およびポリシー記憶部３７から供給された取扱方針にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵Ｋｓｃｐで暗号化し、図１３に示すような署名を作成する。ステップＳ２５７において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、ポリシー記憶部３７から供給される取扱方針、およびステップＳ２５６で生成した署名を含んだ、図１３に示す

ようなコンテンツプロバイダセキュアコンテナを作成する。

【０１８４】

ステップＳ２５８において、コンテンツプロバイダ２の相互認証部３９は、サービスプロバイダ３の相互認証部４５と相互認証する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２５９において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、サービスプロバイダ３に、コンテンツプロバイダセキュアコンテナに、予め認証局から発行してもらった証明書を付して送信し、処理を終了する。

【０１８５】

以上のように、コンテンツプロバイダ２は、サービスプロバイダ３に、コンテンツプロバイダセキュアコンテナを送信する。

【０１８６】

コンテンツ鍵Ｋｃｏと共に取扱方針を配送用鍵Ｋｄで暗号化する例の場合の、コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する他の処理の詳細を、図５６のフローチャートを用いて説明する。ステップＳ２７１乃至ステップＳ２７４の処理は、図５５のステップＳ２５１乃至ステップＳ２５４の処理とそれぞれ同様であり、その説明は省略する。ステップＳ２７５において、コンテンツプロバイダ２の暗号化部３６は、図４０のステップＳ２１の処理により、EMDサービスセンタ１から供給されている配送用鍵Ｋｄを用いて、DESなどの所定の方式で、コンテンツ鍵Ｋｃｏおよびポリシー記憶部３７から供給される取扱方針を暗号化する。

【０１８７】

ステップＳ２７６において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、および暗号化された取扱方針にハッシュ関数を適用しハッシュ値を算出し、自分自身の秘密鍵Ｋｓｃｐで暗号化し、図２５に示すような署名を作成する。ステップＳ２７７において、コンテンツプロバイダ２のセキュアコンテナ作成部３８は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、暗号化された取扱方針、および署名を含んだ、図２５に示すようなコンテンツプロバイダセキュアコン

テナを作成する。ステップＳ２７８およびステップＳ２７９の処理は、図５５のステップＳ２５８およびステップＳ２５９の処理とそれぞれ同様であり、その説明は省略する。

【０１８８】

このように、コンテンツプロバイダ２は、サービスプロバイダ３に、暗号化された取扱方針を含むコンテンツプロバイダセキュアコンテナを送信する。

【０１８９】

次に、図３９のステップＳ１５に対応する、サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理の詳細を図５７のフローチャートを用いて説明する。ステップＳ２９１において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダ２のセキュアコンテナ作成部３８から送信されたコンテンツプロバイダセキュアコンテナに付された証明書に含まれる署名を確認し、証明書の改竄がなければ、コンテンツプロバイダ２の公開鍵Ｋｐｃｐを取り出す。証明書の署名の確認は、図４４のステップＳ８３における処理と同様であるので、その説明は省略する。

【０１９０】

ステップＳ２９２において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダ２のセキュアコンテナ作成部３８から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ２の公開鍵Ｋｐｃｐで復号し、得られたハッシュ値が、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、および取扱方針にハッシュ関数を適用し得られたハッシュ値と一致することを確認し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。改竄が発見された場合は、処理を終了する。

【０１９１】

コンテンツプロバイダセキュアコンテナに改竄がない場合、ステップＳ２９３において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダセキュアコンテナから取扱方針を取り出す。ステップＳ２５４において、サービスプロバイダ３の値付け部４２は、取扱方針を基に、図１７で説明した価格情報を作成する。ステップＳ２９５において、サービスプロバイダ３のセキュアコンテナ

作成部４４は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、価格情報、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵Ｋｃｏ、取扱方針、および価格情報にハッシュ関数を適用して得られたハッシュ値を、自分自身の秘密鍵Ｋｓｓｐで暗号化し、得られた値を署名として図１５に示すようなサービスプロバイダセキュアコンテナを作成する。

【０１９２】

ステップＳ２９６において、サービスプロバイダ３の相互認証部４５は、レシーバ５１の相互認証モジュール７１と相互認証する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップＳ２９７において、サービスプロバイダ３のセキュアコンテナ作成部４４は、レシーバ５１の通信部６１に、証明書を付したサービスプロバイダセキュアコンテナを送信し、処理を終了する。

【０１９３】

このように、サービスプロバイダ３は、レシーバ５１にサービスプロバイダセキュアコンテナを送信する。

【０１９４】

コンテンツプロバイダ２において、取扱方針が配送用鍵Ｋｄで暗号化され、かつ、サービスプロバイダ３が取扱制御情報を作成する例の場合の、サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理の詳細を、図５８のフローチャートを用いて説明する。ステップＳ３１１およびステップＳ３１２の処理は、図５７のステップＳ２９１およびステップＳ２９２の処理とそれぞれ同様であるので、その説明は省略する。ステップＳ３１３において、サービスプロバイダ３の値付け部４２は、コンテンツプロバイダセキュアコンテナに含まれる暗号化された取扱方針を復号する。ステップＳ３１４において、サービスプロバイダ３の値付け部４２は、取扱方針を基に、図２３で説明した取扱制御情報を作成する。ステップＳ３１５乃至ステップＳ３１８の処理は、図５７のステップＳ２９４およびステップＳ２９７の処理とそれぞれ同様であるので、その説明は省略する。

【０１９５】

このように、サービスプロバイダ３は、レシーバ５１に暗号化された取扱方針を含むサービスプロバイダセキュアコンテナを送信する。

【０１９６】

ユーザネットワーク５が図１０または図１１の構成を有するときの、図３９のステップＳ１６に対応する、適正なサービスプロバイダセキュアコンテナを受信した後の、レシーバ５１の課金処理の詳細を、図５９のフローチャートを用いて説明する。ステップＳ３３１において、レシーバ５１の復号／暗号化モジュール７４は、配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを復号できるか否かを判定し、配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを復号できないと判定された場合、ステップＳ３３２で、レシーバ５１は、図５３で説明した配送用鍵Ｋｄの受け取り処理を実行し、ステップＳ３３３に進む。ステップＳ３３１において、配送用鍵Ｋｄでコンテンツ鍵Ｋｃｏを復号できると判定された場合、手続は、ステップＳ３３２をスキップし、ステップＳ３３３に進む。ステップＳ３３３において、レシーバ５１の復号ユニット９１は、図３９のステップＳ１３の処理により、記憶モジュール７３に記憶されている配送用鍵Ｋｄで、コンテンツ鍵Ｋｃｏを復号する。

【０１９７】

ステップＳ３３４において、レシーバ５１の課金処理モジュール７２は、サービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報を取り出し、図１９および図２０で説明した課金情報および使用許諾条件情報を生成する。ステップＳ３３５において、レシーバ５１の課金処理モジュール７２は、記憶モジュール７３に記憶している課金情報およびステップＳ３３４で算出された課金情報から、現在の課金が課金の上限以上であるか否かを判定し、現在の課金が課金の上限以上であると判定された場合、ステップＳ３３６に進み、レシーバ５１は図５３で説明した配送用鍵Ｋｄの受け取り処理を実行し、新たな配送用鍵Ｋｄを受け取り、ステップＳ３３７に進む。ステップＳ３３５において、現在の課金が課金の上限未満であると判定された場合、ステップＳ３３６はスキップされ、ステップＳ３３７に進む。

【０１９８】

ステップＳ３３７において、レシーバ５１の課金処理モジュール７２は、記憶モジュール７３に課金情報を記憶させる。ステップＳ３３８において、レシーバ５１の課金処理モジュール７２は、ステップＳ３３４にて生成した使用許諾条件情報をHDD５２に記録する。ステップＳ３３９において、レシーバ５１のSAM６２は、HDD５２にサービスプロバイダセキュアコンテナから取り出した取扱方針を記録させる。

【０１９９】

ステップＳ３４０において、レシーバ５１の復号／暗号化モジュール７４は、使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。ステップＳ３４１において、レシーバ５１の記憶モジュール７３は、使用許諾条件情報のハッシュ値を記憶する。記憶モジュール７３に保存用鍵Ｋｓａｖｅが記憶されていない場合、ステップＳ３４２において、レシーバ５１の乱数発生ユニット９２は、保存用鍵Ｋｓａｖｅである乱数を発生し、ステップＳ３４３に進む。記憶モジュール７３に保存用鍵Ｋｓａｖｅが記憶されている場合、ステップＳ３４２はスキップされ、ステップＳ３４３に進む。

【０２００】

ステップＳ３４３において、レシーバ５１の暗号化ユニット９３は、コンテンツ鍵Ｋｃｏを保存用鍵Ｋｓａｖｅで暗号化する。ステップＳ３４４において、レシーバ５１のSAM６２は、暗号化されたコンテンツ鍵ＫｃｏをHDD５２に記憶させる。記憶モジュール７３に保存用鍵Ｋｓａｖｅが記憶されていない場合、ステップＳ３４５において、レシーバ５１の復号／暗号化モジュール７４は、保存用鍵Ｋｓａｖｅを記憶モジュール７３に記憶させ、処理は終了する。記憶モジュール７３に保存用鍵Ｋｓａｖｅが記憶されている場合、ステップＳ３４５はスキップされ、処理は終了する。

【０２０１】

以上のように、レシーバ５１は、課金情報を記憶モジュール７３に記憶すると共に、コンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、再度、コンテンツ鍵Ｋｃｏを保存用鍵Ｋｓａｖｅで暗号化し、HDD５２に記録させる。保存用鍵Ｋｓａｖｅ

は、記憶モジュール７３に記憶される。

【０２０２】

レコーダ５３も、同様の処理で、課金情報をSAM６６内の記憶モジュールに記憶すると共に、コンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、再度、コンテンツ鍵Ｋｃｏを保存用鍵Ｋｓａｖｅで暗号化し、HDD５２に記録させる。保存用鍵Ｋｓａｖｅは、SAM６６内の記憶モジュールに記憶される。

【０２０３】

ユーザネットワーク５が図３０の構成を有し、記憶モジュール７３に検査値を記憶する場合の、図３９のステップＳ１５およびステップＳ１６に対応する、レシーバ５１の、適正なサービスプロバイダセキュアコンテナを受信し、課金する処理の詳細を、図６０のフローチャートを用いて説明する。ステップＳ３６１において、レシーバ５１の相互認証モジュール７１は、通信部６１を介して、サービスプロバイダ３の相互認証部４４と相互認証し、相互認証できたとき、通信部６１は、相互認証したサービスプロバイダ３から、サービスプロバイダセキュアコンテナを受信する。相互認証できなかった場合、処理は終了する。ステップＳ３６２において、通信部６１は、ステップＳ３６１で相互認証したサービスプロバイダ３から、公開鍵証明書を受信する。

【０２０４】

ステップＳ３６３において、復号／暗号化モジュール６２は、ステップＳ３６１で受信したサービスプロバイダセキュアコンテナに含まれる署名データを検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了する。ステップＳ３６４において、レシーバ５１は、図示せぬ表示部に受信したサービスプロバイダセキュアコンテナに含まれる取扱情報および価格情報を表示し、ユーザは、コンテンツの再生またはコピーなど、購入の内容を決定し、レシーバ５１にその内容を指示する。ステップＳ３６５において、レシーバ５１の課金処理モジュール７２は、取扱情報および価格情報、並びに購入の内容を基に、課金情報および使用許諾条件情報を生成する。

【０２０５】

ステップＳ３６６において、SAM６２は、サービスプロバイダセキュアコンテ

ナに含まれるコンテンツ鍵Ｋｃｏで暗号化されているコンテンツをHDD５２に記録させる。ステップＳ３６７において、復号／暗号化ユニット７４の復号ユニット９１は、サービスプロバイダセキュアコンテナに含まれる配送用鍵Ｋｄで暗号化されているコンテンツ鍵Ｋｃｏを、図４５のステップＳ１１０または図５３のステップＳ２１０で記憶モジュール７３に記憶している配送用鍵Ｋｄで復号する。ステップＳ３６８において、暗号化ユニット９３は、ステップＳ３６７で復号されたコンテンツ鍵を記憶モジュール７３に記憶している保存用鍵Ｋｓａｖｅで暗号化する。

【０２０６】

ステップＳ３６９において、データ検査モジュール１１４は、外部記憶部１１３の、空きを有する鍵データブロックを検索する。ステップＳ３７０において、データ検査モジュール１１４は、ステップＳ３６９で検索した鍵データブロックに記憶されているデータ（コンテンツ鍵Ｋｃｏ、コンテンツIDなどのデータ）にハッシュ関数を適用し、ハッシュ値を得る。ステップＳ３７１において、データ検査モジュール１１４は、ステップＳ３７０で得られたハッシュ値と、記憶モジュール７３に記憶されている、ステップＳ３６９で検索された鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップＳ３７２に進み、SAM６２は、ステップＳ３６８にて暗号化されたコンテンツ鍵Ｋｃｏを、外部記憶部１１３の空きを有する鍵データブロックに記憶させる。

【０２０７】

ステップＳ３７３において、復号／暗号化モジュール７４は、外部記憶部１１３の、コンテンツ鍵Ｋｃｏを記憶させた鍵データブロックに記憶しているデータにハッシュ関数を適用し、ハッシュ値を得る。ステップＳ３７４において、復号／暗号化モジュール７４は、ステップＳ３７３にて算出したハッシュ値を、記憶モジュール７３の、コンテンツ鍵Ｋｃｏを記憶させた鍵データブロックに対応する検査値に上書きする。ステップＳ３７５において、課金モジュール７２は、ステップＳ３６５で作成した課金情報を記憶モジュール７３に記憶させ、処理は終了する。

【０２０８】

ステップＳ３７１において、ステップＳ３７０で得られたハッシュ値と、記憶モジュール７３に記憶されている、ステップＳ３６９で検索された鍵データブロックに対応する検査値とを比較し、一致しないと判定された場合、その鍵データブロックのデータは改竄されているので、手続きは、ステップＳ３７６に進み、データ検査モジュール１１４は、外部記憶部１１３の全ての鍵データブロックを調べたか否かを判定し、外部記憶部１１３の全ての鍵データブロックを調べていないと判定された場合、ステップＳ３７７に進み、データ検査モジュール１１４は、外部記憶部１１３の、他の空きを有する鍵データブロックを検索し、ステップＳ３７０に戻り、処理を繰り返す。

【０２０９】

ステップＳ３７６において、外部記憶部１１３の全ての鍵データブロックを調べたと判定された場合、コンテンツ鍵Ｋｃｏを記憶できる鍵データブロックは無いので、処理は終了する。

【０２１０】

このように、図３０のレシーバ５１は、外部記憶部１１３のコンテンツ鍵Ｋｃｏ等が記憶されている鍵データブロックの改竄を検査し、改竄のない鍵データブロックのみに、新たなコンテンツ鍵Ｋｃｏを記憶する。

【０２１１】

ユーザネットワーク５が図３０の構成を有し、外部記憶部１１３に検査値を記憶する場合の、図３９のステップＳ１５およびステップＳ１６に対応する、レシーバ５１の、適正なサービスプロバイダセキュアコンテナを受信し、課金する処理の詳細を、図６１のフローチャートを用いて説明する。ステップＳ３９１乃至ステップＳ４００の処理は、図６０のステップＳ３６１乃至ステップＳ３７０の処理とそれぞれ同様であり、その説明は省略する。

【０２１２】

ステップＳ４０１において、復号ユニット９１は、外部記憶部１１３に記憶されている、ステップＳ３９９で検索した鍵データブロックに対応する検査値を、記憶モジュール７３に記憶する検査用鍵Ｋｃｈで復号する。ステップＳ４０２に

おいて、データ検査モジュール１１４は、ステップＳ４００で得られたハッシュ値と、ステップＳ４０１で復号された検査値とを比較し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、手続きは、ステップＳ４０３に進む。

【０２１３】

ステップＳ４０３およびステップＳ４０４の処理は、図６０のステップＳ３７２およびステップＳ３７３の処理とそれぞれ同様であり、その説明は省略する。

【０２１４】

ステップＳ４０５において、暗号化ユニット９３は、ステップＳ４０４において得られたハッシュ値を、記憶モジュール７３に記憶する検査用鍵Ｋｃｈで暗号化する。ステップＳ４０６において、復号／暗号化モジュール７４は、ステップＳ４０５にて暗号化したハッシュ値を、記憶モジュール７３の、コンテンツ鍵Ｋｃｏを記憶させた鍵データブロックに対応する検査値に上書きする。

【０２１５】

ステップＳ４０７乃至ステップＳ４０９の処理は、図６０のステップＳ３７５乃至ステップＳ３７７の処理とそれぞれ同様であり、その説明は省略する。

【０２１６】

このように、図６１に示す処理においても、図３０のレシーバ５１は、外部記憶部１１３のコンテンツ鍵Ｋｃｏ等が記憶されている鍵データブロックの改竄を検査し、改竄のない鍵データブロックのみに、新たなコンテンツ鍵Ｋｃｏを記憶する。

【０２１７】

次に、ユーザネットワーク５が図３０の構成を有する場合の、MDドライブ５４から供給される暗号化されていないコンテンツを、暗号化し、記録する処理の詳細を、図６２のフローチャートを用いて説明する。ステップＳ４２１において、SAM６２の乱数発生ユニット９２は、乱数を生成し、コンテンツ鍵Ｋｃｏとする。ステップＳ４２２において、通信部６１は、MDドライブ５４から、MDドライブ５４に装着されているMDが記録するコンテンツを受信する。ステップＳ４２３において、SAM６２の暗号化ユニット９３は、ステップＳ４２２で受信したコンテ

ンツを、ステップＳ４２１で生成したコンテンツ鍵Ｋｃｏで暗号化する。ステップＳ４２４において、SAM６２は、暗号化されたコンテンツをHDD５２に記録させる。ステップＳ４２５において、SAM６２の暗号化ユニット９３は、コンテンツ鍵Ｋｃｏを記憶モジュール７３に記憶している保存用鍵Ｋｓａｖｅで暗号化する。

【０２１８】

ステップＳ４２６乃至ステップＳ４３４の処理は、図６０のステップＳ３６９乃至ステップＳ３７７の処理とそれぞれ同等であり、その説明は、省略する。

【０２１９】

このように、レシーバ５１は、MDドライブ５４から供給される暗号化されていないコンテンツを、暗号化し、HDD５２に記録する。

【０２２０】

図３９のステップＳ１７に対応するレシーバ５１がコンテンツを再生する処理の詳細を、図６３のフローチャートを用いて説明する。ステップＳ４５１において、レシーバ５１の復号／暗号化モジュール７４は、HDD５２から、図５９のステップＳ３３８で記憶した使用許諾条件情報およびステップＳ３４４で記憶した暗号化されたコンテンツ鍵Ｋｃｏを読み出す。ステップＳ４５２において、レシーバ５１の復号／暗号化モジュール７４は、使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。

【０２２１】

ステップＳ４５３において、レシーバ５１の復号／暗号化モジュール７４は、ステップＳ４５２において算出されたハッシュ値が、図５９のステップＳ３４０で記憶モジュール７３に記憶されたハッシュ値と一致するか否かを判定し、ステップＳ４５２において算出されたハッシュ値が、記憶モジュール７３に記憶されたハッシュ値と一致すると判定された場合、ステップＳ４５４に進み、使用回数の値などの使用許諾条件情報に含まれる所定の情報を更新する。ステップＳ４５５において、レシーバ５１の復号／暗号化モジュール７４は、更新した使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。ステップＳ４５６において、レシーバ５１の記憶モジュール７３は、ステップＳ４５５で算出した使用

許諾条件情報のハッシュ値を記憶する。ステップＳ４５７において、レシーバ５１の復号／暗号化モジュール７４は、HDD５２に更新した使用許諾条件情報を記録させる。

【０２２２】

ステップＳ４５８において、SAM６２の相互認証モジュール７１と伸張部６３の相互認証モジュール７５は、相互認証し、SAM６２および伸張部６３は、一時鍵Ｋｔｅｍｐを記憶する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数Ｒ１、Ｒ２、またはＲ３が、一時鍵Ｋｔｅｍｐとして用いられる。ステップＳ４５９において、復号／暗号化モジュール７４の復号ユニット９１は、図５９のステップＳ３４４にてHDD５２に記録されたコンテンツ鍵Ｋｃｏを、記憶モジュール７３に記憶された保存用鍵Ｋｓａｖｅで復号する。ステップＳ４６０において、復号／暗号化モジュール７４の暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで暗号化する。ステップＳ４６１において、SAM６２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを伸張部６３に送信する。

【０２２３】

ステップＳ４６２において、伸張部６３の復号モジュール７６は、コンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号する。ステップＳ４６３において、SAM６２は、HDD５２に記録されたコンテンツを読み出し、伸張部６３に送信する。ステップＳ４６４において、伸張部６３の復号モジュール７７は、コンテンツをコンテンツ鍵Ｋｃｏで復号する。ステップＳ４６５において、伸張部６３の伸張モジュール７８は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップＳ４６６において、伸張部６３のウォータマーク付加モジュール７９は、伸張されたコンテンツにレシーバ５１を特定する所定のウォータマークを挿入する。ステップＳ４６７において、レシーバ５１は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【０２２４】

ステップＳ４５３において、ステップＳ４５２において算出されたハッシュ値

が、記憶モジュール７３に記憶されたハッシュ値と一致しないと判定された場合、ステップＳ４６８において、SAM６２は、図示せぬ表示装置にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

【０２２５】

このように、レシーバ５１は、コンテンツを再生する。

【０２２６】

図６４は、図１１の構成を有するユーザホームネットワーク５において、レシーバ５１がデコーダ５６にコンテンツを再生させる処理を説明するフローチャートである。ステップＳ４８１乃至ステップＳ４８７の処理は、図６３のステップＳ４５１乃至ステップＳ４５７の処理とそれぞれ同様であるので、その説明は省略する。

【０２２７】

ステップＳ４８８において、SAM６２の相互認証モジュール７１とデコーダ５６の相互認証モジュール１０１は、相互認証し、一時鍵Ｋｔｅｍｐが共有される。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数Ｒ１、Ｒ２、またはＲ３が、一時鍵Ｋｔｅｍｐとして用いられる。ステップＳ４８９において、復号／暗号化モジュール７４の復号ユニット９１は、HDD５２に記録されたコンテンツ鍵Ｋｃｏを、記憶モジュール７３に記憶された保存用鍵Ｋｓａｖｅで復号する。ステップＳ４９０において、復号／暗号化モジュール７４の暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで暗号化する。ステップＳ４９１において、SAM６２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏをデコーダ５６に送信する。

【０２２８】

ステップＳ４９２において、デコーダ５６の復号モジュール１０２は、コンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号する。ステップＳ４９３において、SAM６２は、HDD５２に記録されたコンテンツを読み出し、デコーダ５６に送信する。ステップＳ４９４において、デコーダ５６の復号モジュール１０３は、コンテンツをコンテンツ鍵Ｋｃｏで復号する。ステップＳ４９５において、デコーダ５

６の伸張モジュール１０４は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップＳ４９６において、デコーダ５６のウォータマーク付加モジュール１０５は、伸張されたコンテンツにデコーダ５６を特定する所定のウォータマークを挿入する。ステップＳ４９７において、デコーダ５６は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【０２２９】

ステップＳ４９８の処理は、図６３のステップＳ４６８の処理と同様であるので、その説明は省略する。

【０２３０】

以上のように、ユーザホームネットワークが図１１に示す構成を有する場合、レシーバ５１が受信したコンテンツは、デコーダ５６で再生される。

【０２３１】

続いて、ユーザネットワーク５が図３０の構成を有し、検査値が記憶モジュール７３および記憶部１３５に記憶されているときの、HDD５２に記録されているコンテンツを、レシーバ５１に装着されているメモリスティック１１１に移動する処理を、図６５および図６６のフローチャートを参照して説明する。ステップＳ５１１において、レシーバ５１の相互認証モジュール７１は、レシーバ５１に装着されているメモリスティック１１１の相互認証部１３３と相互認証し、一時鍵Ｋｔｅｍｐを共有する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０２３２】

ステップＳ５１２において、レシーバ５１は、HDD５２からコンテンツに関するデータを検索し、図示せぬ表示部に表示し、ユーザは、メモリスティック１１１に移動するコンテンツを選択し、レシーバ５１に所定のデータを図示せぬスイッチで、入力する。ステップＳ５１３において、レシーバ５１のSAM６２は、選択されたコンテンツに対応するコンテンツ鍵を、外部記憶部１１３から検索する。ステップＳ５１４において、レシーバ５１のデータ検査モジュール１１４は、移動するコンテンツに対応するコンテンツ鍵Ｋｃｏを記憶する、外部記憶部１１３の鍵データブロックに記憶しているデータ（コンテンツ鍵Ｋｃｏ、コンテンツ

IDなどのデータ）に、ハッシュ関数を適用し、ハッシュ値を得る。ステップＳ５１５において、データ検査モジュール１１４は、ステップＳ５１４で得られたハッシュ値と、記憶モジュール７３に記憶されている、コンテンツ鍵Ｋｃｏを記憶している鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップＳ５１６に進み、レシーバ５１の通信部６１は、メモリスティック１１１の通信部１３１に書き込み要求コマンドおよびコンテンツIDを送信し、メモリスティック１１１の通信部１３１は、書き込み要求コマンドおよびコンテンツIDを受信する。

【０２３３】

ステップＳ５１７において、レシーバ５１の通信部６１は、メモリスティック１１１の通信部１３１にステップＳ５１２で選択されたコンテンツを送信し、メモリスティック１１１の通信部１３１は、コンテンツを受信する。ステップＳ５１８において、メモリスティック１１１のメモリコントローラ１３２は、通信部１３１が受信したコンテンツを、情報記憶ブロック１２２に、暗号化データ１４４として記憶させる。

【０２３４】

ステップＳ５１９において、レシーバ５１の復号ユニット９１は、コンテンツ鍵Ｋｃｏを記憶モジュール７３に記憶している保存用鍵Ｋｓａｖｅで復号し、暗号化ユニット９３は、復号したコンテンツ鍵Ｋｃｏを、一時鍵Ｋｔｅｍｐで再度、暗号化し、SAM６２内の図示せぬレジスタに一時的に記憶する。ステップＳ５２０において、SAM６２は、移動するコンテンツに対応する、外部記憶部１１３に記憶されているコンテンツ鍵Ｋｃｏを削除する。ステップＳ５２１において、レシーバ５１の復号／暗号化モジュール７４は、移動するコンテンツに対応するコンテンツ鍵Ｋｃｏを削除した、外部記憶部１１３の鍵データブロックに記憶しているデータに、ハッシュ関数を適用し、ハッシュ値を得る。ステップＳ５２２において、復号／暗号化モジュール７４は、ステップＳ５２１にて算出したハッシュ値を、記憶モジュール７３の、コンテンツ鍵Ｋｃｏを削除した鍵データブロックに対応する検査値に上書きする。

【０２３５】

ステップＳ５２３において、レシーバ５１の通信部６１は、コンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報を、メモリスティック１１１の通信部１３１に送信し、メモリスティック１１１の通信部１３１は、コンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報を受信する。ステップＳ５２４において、メモリスティック１１１の復号部１３６は、受信部１３１が受信したコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、暗号化部１３４は、復号したコンテンツ鍵Ｋｃｏを記憶部１３５が記憶する保存用鍵Ｋｓａｖｅで暗号化し、制御ブロック１２１内の図示せぬレジスタに一時的に記憶させる。

【０２３６】

ステップＳ５２５において、データ検査部１３８は、鍵データ１４３の、空きを有する鍵データブロックを検索する。ステップＳ５２６において、データ検査部１３８は、ステップＳ５２５で検索した鍵データブロックに記憶されているデータ（コンテンツ鍵Ｋｃｏ、コンテンツIDなどのデータ）にハッシュ関数を適用し、ハッシュ値を得る。ステップＳ５２７において、データ検査部１３８は、ステップＳ５２６で算出したハッシュ値と、記憶部１３５に記憶されている、ステップＳ５２５で検索された鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致していると判定された場合、ステップＳ５２８に進み、メモリコントローラ１３２は、レジスタに一時的に記憶されているコンテンツ鍵Ｋｃｏを、鍵データ１４３の空きのある鍵データブロックに記憶させる。

【０２３７】

ステップＳ５２９において、データ検査部１３８は、鍵データ１４３の、コンテンツ鍵Ｋｃｏを記憶させた鍵データブロックに記憶しているデータにハッシュ関数を適用し、ハッシュ値を得る。ステップＳ５３０において、データ検査部１３８は、ステップＳ５２９にて算出したハッシュ値を、記憶部１３５の、コンテンツ鍵Ｋｃｏを記憶させた鍵データブロックに対応する検査値に上書きする。

【０２３８】

ステップＳ５３１において、メモリスティック１１１の通信部１３１は、レシーバ５１の通信部６１に、受信完了信号を送信し、レシーバ５１の通信部６１は

、受信完了信号を受信する。ステップＳ５３２において、レシーバ５１のSAM６２は、HDD６２からコンテンツを削除させ、コンテンツ鍵Ｋｃｏをレジスタから削除し、処理は終了する。

【０２３９】

ステップＳ５２７において、ステップＳ５２６で得られたハッシュ値と、記憶部１３５に記憶されている、ステップＳ５２３で検索された鍵データブロックに対応する検査値とを比較し、一致しないと判定された場合、その鍵データブロックのデータは改竄されているので、手続きは、ステップＳ５３３に進み、データ検査部１３５は、鍵データ１４３の全ての鍵データブロックを調べたか否かを判定し、鍵データ１４３の全ての鍵データブロックを調べていないと判定された場合、ステップＳ５３４に進み、データ検査部１３５は、鍵データ１４３の、他の空きを有する鍵データブロックを検索し、ステップＳ５２６に戻り、処理を繰り返す。

【０２４０】

ステップＳ５３３において、鍵データ１４３の全ての鍵データブロックを調べたと判定された場合、コンテンツ鍵Ｋｃｏを記憶できる鍵データブロックは無いので、処理は終了する。

【０２４１】

ステップＳ５１５において、データ検査モジュール１１４は、ステップＳ５１４で得られたハッシュ値と、記憶モジュール７３に記憶されている、コンテンツ鍵Ｋｃｏを記憶している鍵データブロックに対応する検査値が一致しないと判定された場合、移動しようとしているコンテンツは改竄されているので、処理は終了する。

【０２４２】

以上のように、HDD６２に記憶されているコンテンツは、メモリスティック１１１に移動される。

【０２４３】

ユーザネットワーク５が図３０の構成を有し、検査値が外部記憶部１１３および鍵データ１４３に記憶されているときの、HDD５２に記録されているコンテン

ツを、レシーバ５１に装着されているメモリスティック１１１に移動する処理を、図６７および図６８のフローチャートを参照して説明する。ステップＳ５５１乃至ステップＳ５５４の処理は、図６５のステップＳ５１１乃至ステップＳ５１４の処理とそれぞれ同様なので、その説明は省略する。

【０２４４】

ステップＳ５５５において、データ検査モジュール１１４は、コンテンツ鍵Ｋｃｏを記憶している鍵データブロックに対応する検査値を記憶モジュール７３が記憶する検査用鍵Ｋｃｈで復号する。ステップＳ５５６において、データ検査モジュール１１４は、ステップＳ５５４で得られたハッシュ値と、ステップＳ５５５で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップＳ５５７に進む。

【０２４５】

ステップＳ５５７乃至ステップＳ５６２の処理は、図６５のステップＳ５１６乃至ステップＳ５２１の処理とそれぞれ同様なので、その説明は省略する。

【０２４６】

ステップＳ５６３において、暗号化ユニット９３は、ステップＳ５６２で算出されたハッシュ値を、記憶モジュール７３に記憶する検査用鍵Ｋｃｈで暗号化する。ステップＳ５６４において、復号／暗号化モジュール７４は、ステップＳ５６３にて暗号化したハッシュ値を、外部記憶部１１３の、コンテンツ鍵Ｋｃｏを削除した鍵データブロックに対応する検査値に上書きする。

【０２４７】

ステップＳ５６５乃至ステップＳ５６８の処理は、図６５または図６６のステップＳ５２３乃至ステップＳ５２６の処理とそれぞれ同様なので、その説明は省略する。

【０２４８】

ステップＳ５６９において、復号部１３６は、ステップＳ５６７で検索した鍵データブロックに対応する検査値を記憶部１３５が記憶する検査用鍵Ｋｃｈで復号する。ステップＳ５７０において、データ検査部１３８は、ステップＳ５６８

で得られたハッシュ値と、ステップＳ５６９で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップＳ５７１に進む。

【０２４９】

ステップＳ５７１およびステップＳ５７２の処理は、図６６のステップＳ５２８およびステップＳ５２９の処理と、それぞれ同様なので、その説明は省略する。

【０２５０】

ステップＳ５７３において、データ検査部１３８は、ステップＳ５７２で算出されたハッシュ値を、記憶部１３５に記憶している検査用鍵Ｋｃｈで暗号化する。ステップＳ５７４において、データ検査部１３８は、ステップＳ５７３にて暗号化したハッシュ値を、鍵データ１４３の、コンテンツ鍵Ｋｃｏを記憶させた鍵データブロックに対応する検査値に上書きする。

【０２５１】

ステップＳ５７５乃至ステップＳ５７８の処理は、図６６のステップＳ５３１乃至ステップＳ５３４の処理と、それぞれ同様なので、その説明は省略する。

【０２５２】

ステップＳ５５６において、データ検査モジュール１１４は、ステップＳ５５４で得られたハッシュ値と、ステップＳ５５５で復号した検査値が一致しないと判定された場合、移動しようとしているコンテンツは改竄されているので、処理は終了する。

【０２５３】

このように、HDD６２に記憶されているコンテンツは、メモリスティック１１１に移動される。

【０２５４】

次に、ユーザネットワーク５が図３０の構成を有し、検査値が記憶モジュール７３および記憶部１３５に記憶されているときの、レシーバ５１に装着されているメモリスティック１１１に記憶されているコンテンツを、HDD５２に移動する処理を、図６９および図７０のフローチャートを参照して説明する。ステップＳ

５９１において、レシーバ５１の相互認証モジュール７１は、レシーバ５１に装着されているメモリスティック１１１の相互認証部１３３と相互認証し、一時鍵Ｋｔｅｍｐを共有する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０２５５】

ステップＳ５９２において、レシーバ５１は、通信部６１を介して、メモリスティック１１１のデータ検索用テーブルからコンテンツに関するデータを検索し、図示せぬ表示部に表示し、ユーザは、HDD５２に移動するコンテンツを選択し、レシーバ５１に所定のデータを図示せぬスイッチで、入力する。ステップＳ５９３において、レシーバ５１の通信部６１は、メモリスティック１１１の通信部１３１に移動要求コマンドおよびコンテンツIDを送信し、メモリスティック１１１の通信部１３１は、移動要求コマンドおよびコンテンツIDを受信する。

【０２５６】

ステップＳ５９４において、メモリスティック１１１のメモリコントローラ１３２は、受信したコンテンツIDに対応したコンテンツ鍵Ｋｃｏを、鍵データ１４３から検索する。ステップＳ５９５において、データ検査部１３８は、コンテンツIDに対応したコンテンツ鍵Ｋｃｏを記憶している鍵データブロックに記憶されているデータ（コンテンツ鍵Ｋｃｏ、コンテンツIDなどのデータ）にハッシュ関数を適用し、ハッシュ値を得る。ステップＳ５９６において、データ検査部１３８は、ステップＳ５９５で算出したハッシュ値と、記憶部１３５に記憶されている、コンテンツIDに対応したコンテンツ鍵Ｋｃｏを記憶している鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致していると判定された場合、コンテンツ鍵Ｋｃｏなどに改竄はないので、ステップＳ５９７に進み、メモリコントローラ１３２は、データ検索用テーブル１４１を参照して、コンテンツIDに対応したコンテンツを暗号化データ１４４から検索する。

【０２５７】

ステップＳ５９８において、メモリスティック１１１の通信部１３１は、レシーバ５１の通信部６１にステップＳ５９７で検索されたコンテンツを送信し、レシーバ５１の通信部６１は、コンテンツを受信する。ステップＳ５９９において

、SAM６２は、受信部６１が受信したコンテンツをHDD５２に記憶させる。

【０２５８】

ステップＳ６００において、メモリスティック１１１の復号部１３６は、コンテンツ鍵Ｋｃｏを記憶部１３５に記憶している保存用鍵Ｋｓａｖｅで復号し、暗号化部１３４は、復号したコンテンツ鍵Ｋｃｏを、一時鍵Ｋｔｅｍｐで再度、暗号化し、制御ブロック１２１内の図示せぬレジスタに一時的に記憶する。ステップＳ６０１において、メモリコントローラ１３２は、移動するコンテンツに対応する、鍵データ１４３に記憶されているコンテンツ鍵Ｋｃｏを削除する。ステップＳ６０２において、制御ブロック１２１のデータ検査部１３８は、移動するコンテンツに対応するコンテンツ鍵Ｋｃｏを削除した、鍵データ１４３の鍵データブロックに記憶しているデータに、ハッシュ関数を適用し、ハッシュ値を得る。ステップＳ６０３において、データ検査部１３８は、ステップＳ６０２にて算出したハッシュ値を、鍵データ１４３の、コンテンツ鍵Ｋｃｏを削除した鍵データブロックに対応する検査値に上書きする。

【０２５９】

ステップＳ６０４において、メモリスティック１１１の通信部１３１は、コンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報を、レシーバ５１の通信部６１に送信し、レシーバ５１の通信部６１は、コンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報を受信する。ステップＳ６０５において、レシーバ５１のデータ検査モジュール７３は、外部記憶部１１３の、空きを有する鍵データブロックを検索する。ステップＳ６０６において、データ検査モジュール１１４は、ステップＳ６０５で検索した鍵データブロックに記憶されているデータにハッシュ関数を適用し、ハッシュ値を得る。ステップＳ６０７において、データ検査モジュール１１４は、ステップＳ６０６で得られたハッシュ値と、記憶モジュール７３に記憶されている、ステップＳ６０５で検索された鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップＳ６０８に進み、レシーバ５１の復号ユニット９１は、受信部６１が受信したコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、暗号化ユニット９３は、復号した

コンテンツ鍵Ｋｃｏを記憶モジュール７３が記憶する保存用鍵Ｋｓａｖｅで暗号化する。ステップＳ６０９に進み、SAM６２は、ステップＳ６０７にて暗号化されたコンテンツ鍵Ｋｃｏを、外部記憶部１１３の空きを有する鍵データブロックに記憶させる。

【０２６０】

ステップＳ６１０において、復号／暗号化モジュール７４は、外部記憶部１１３の、コンテンツ鍵Ｋｃｏを記憶させた鍵データブロックに記憶しているデータにハッシュ関数を適用し、ハッシュ値を得る。ステップＳ６１１において、復号／暗号化モジュール７４は、ステップＳ６１０にて算出したハッシュ値を、記憶モジュール７３の、コンテンツ鍵Ｋｃｏを記憶させた鍵データブロックに対応する検査値に上書きする。ステップＳ６１２において、レシーバ５１の通信部６１は、メモリスティック１１１の通信部１３１に受信完了信号を送信し、メモリスティック１１１の通信部１３１は、受信完了信号を受信する。ステップＳ６１３において、メモリスティック１１１のメモリコントローラ１３２は、暗号化データ１４４から、送信したコンテンツを削除し、鍵データ１４３から、対応するコンテンツ鍵Ｋｃｏを削除し、処理は終了する。

【０２６１】

ステップＳ６０７において、ステップＳ６０６で得られたハッシュ値と、記憶モジュール７３に記憶されている、ステップＳ６０５で検索された鍵データブロックに対応する検査値とを比較し、一致しないと判定された場合、その鍵データブロックのデータは改竄されているので、手続きは、ステップＳ６１４に進み、データ検査モジュール１１４は、外部記憶部１１３の全ての鍵データブロックを調べたか否かを判定し、外部記憶部１１３の全ての鍵データブロックを調べていないと判定された場合、ステップＳ６１５に進み、データ検査モジュール１１４は、外部記憶部１１３の、他の空きを有する鍵データブロックを検索し、ステップＳ６０６に戻り、処理を繰り返す。

【０２６２】

ステップＳ６１４において、外部記憶部１１３の全ての鍵データブロックを調べたと判定された場合、コンテンツ鍵Ｋｃｏを記憶できる鍵データブロックは無

いので、処理は終了する。

【０２６３】

ステップＳ５９６において、ステップＳ５９５で算出したハッシュ値と、記憶部１３５に記憶されている、コンテンツIDに対応したコンテンツ鍵Ｋｃｏを記憶している鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致していないと判定された場合、送信したいコンテンツのコンテンツ鍵Ｋｃｏなどに改竄があるので、処理は終了する。

【０２６４】

このように、コンテンツは、メモリスティック１１１から、レシーバ５１に移動される。

【０２６５】

ユーザネットワーク５が図３０の構成を有し、検査値が外部記憶部１１３および鍵データ１４３に記憶されているときの、レシーバ５１に装着されているメモリスティック１１１に記憶されているコンテンツを、HDD５２に移動する処理を、図７１および図７２のフローチャートを参照して説明する。ステップＳ６３１乃至ステップＳ６３５の処理は、図６９のステップＳ５９１乃至ステップＳ５９５の処理とそれぞれ同様なので、その説明は省略する。

【０２６６】

ステップＳ６３６において、復号部１３６は、コンテンツ鍵Ｋｃｏを記憶している鍵データブロックに対応する検査値を記憶部１３５が記憶する検査用鍵Ｋｃｈで復号する。ステップＳ６３７において、データ検査部１３８は、ステップＳ６３５で得られたハッシュ値と、ステップＳ６３６で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップＳ６３８に進む。

【０２６７】

ステップＳ６３８乃至ステップＳ６４３の処理は、図６９のステップＳ５９７乃至ステップＳ６０２の処理とそれぞれ同様なので、その説明は省略する。

【０２６８】

ステップＳ６４４において、データ検査部１３８は、ステップＳ６４３で算出

されたハッシュ値を、記憶部１３５に記憶する検査用鍵Ｋｃｈで暗号化する。ステップＳ６４５において、データ検査部１３８は、ステップＳ６４４にて暗号化したハッシュ値を、鍵データ１４３の、コンテンツ鍵Ｋｃｏを削除した鍵データブロックに対応する検査値に上書きする。

【０２６９】

ステップＳ６４６およびステップＳ６４７の処理は、図７０のステップＳ６０４およびステップＳ６０５の処理とそれぞれ同様なので、その説明は省略する。

【０２７０】

ステップＳ６４９において、データ検査モジュール１１４は、ステップＳ６４７で検索した鍵データブロックに対応する検査値を記憶部１３５が記憶する検査用鍵Ｋｃｈで復号する。ステップＳ６５０において、データ検査モジュール１１４は、ステップＳ６４８で得られたハッシュ値と、ステップＳ６４９で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップＳ６５１に進む。

【０２７１】

ステップＳ６５１乃至ステップＳ６５３の処理は、図７０のステップＳ６０８乃至ステップＳ６１０の処理とそれぞれ同様なので、その説明は省略する。

【０２７２】

ステップＳ６５４において、暗号化ユニット９３は、ステップＳ６５５で算出されたハッシュ値を、記憶モジュール７３に記憶している検査用鍵Ｋｃｈで暗号化する。ステップＳ６５５において、復号／暗号化モジュール７４は、ステップＳ６５４にて暗号化したハッシュ値を、外部記憶部１１３の、コンテンツ鍵Ｋｃｏを記憶させた鍵データブロックに対応する検査値に上書きする。

【０２７３】

ステップＳ６５６乃至ステップＳ６５９の処理は、図７０のステップＳ６１２乃至ステップＳ６１５の処理と、それぞれ同様なので、その説明は省略する。

【０２７４】

以上のように、検査値が外部記憶部１１３および鍵データ１４３に記憶されて

いるときでも、コンテンツは、メモリスティック１１１から、レシーバ５１に移動される。

【０２７５】

次に、ユーザネットワーク５が図３０の構成を有し、検査値が記憶部１３５に記憶されているときの、レシーバ５１に装着されているメモリスティック１１１に記憶されているコンテンツを、レシーバ５１が再生する処理を、図７３のフローチャートを参照して説明する。ステップＳ６７１において、SAM６２の相互認証モジュール７１は、レシーバ５１に装着されているメモリスティック１１１の相互認証部１３３と相互認証し、一時鍵Ｋｔｅｍｐを共有する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。コンテンツの再生におけるステップＳ６７１の相互認証で使用される鍵は、図６９に示すコンテンツの移動におけるステップＳ５９１の相互認証で使用する鍵と、異なる鍵を使用してもよい。

【０２７６】

ステップＳ６７２において、レシーバ５１のSAM６２は、通信部６１を介して、メモリスティック１１１のデータ検索用テーブルからコンテンツに関するデータを検索し、図示せぬ表示部に表示させ、ユーザは、再生するコンテンツを選択し、レシーバ５１に所定のデータを図示せぬスイッチで、入力する。ステップＳ６７３において、レシーバ５１のSAM６２は、通信部６１を介して、メモリスティック１１１の通信部１３１に読み出し要求コマンドおよびコンテンツIDを送信し、メモリスティック１１１の通信部１３１は、読み出し要求コマンドおよびコンテンツIDを受信する。

【０２７７】

ステップＳ６７４において、メモリスティック１１１のメモリコントローラ１３２は、受信したコンテンツIDに対応したコンテンツ鍵Ｋｃｏを、鍵データ１４３から検索する。ステップＳ６７５において、データ検査部１３８は、コンテンツIDに対応したコンテンツ鍵Ｋｃｏを記憶している鍵データブロックに記憶されているデータ（コンテンツ鍵Ｋｃｏ、コンテンツIDなどのデータ）にハッシュ関数を適用し、ハッシュ値を得る。ステップＳ６７６において、データ検査部１３

８は、ステップＳ６７５で算出したハッシュ値と、記憶部１３５に記憶されている、コンテンツIDに対応したコンテンツ鍵Ｋｃｏを記憶している鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致していると判定された場合、コンテンツ鍵Ｋｃｏなどに改竄はないので、ステップＳ６７７に進み、メモリコントローラ１３２は、データ検索用テーブル１４１を参照して、コンテンツIDに対応したコンテンツを暗号化データ１４４から検索する。

【０２７８】

ステップＳ６７８において、メモリスティック１１１の通信部１３１は、レシーバ５１の通信部６１にステップＳ６７７で検索されたコンテンツを送信し、レシーバ５１の通信部６１は、コンテンツを受信する。ステップＳ６７９において、メモリスティック１１１の復号部１３６は、コンテンツ鍵Ｋｃｏを記憶部１３５に記憶している保存用鍵Ｋｓａｖｅで復号し、暗号化部１３４は、復号したコンテンツ鍵Ｋｃｏを、一時鍵Ｋｔｅｍｐで再度、暗号化し、制御ブロック１２１内の図示せぬレジスタに一時的に記憶する。ステップＳ６８０において、メモリスティック１１１の通信部１３１は、コンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報を、レシーバ５１のSAM６２に送信し、レシーバ５１のSAM６２は、コンテンツ鍵Ｋｃｏ、コンテンツID、および使用許諾条件情報を受信する。

【０２７９】

ステップＳ６８１において、SAM６２の相互認証モジュール７１は、伸張部６３の相互認証モジュール７５と相互認証し、一時鍵Ｋｔｅｍｐ（ステップＳ６７１で共有する一時鍵Ｋｔｅｍｐとは異なる）を共有する。この認証処理は、図４２乃至図４４を参照して説明した場合と同様であるので、ここでは説明を省略する。

【０２８０】

ステップＳ６８２において、SAM６２の復号ユニット９１は、コンテンツ鍵Ｋｃｏを、メモリスティック１１１と共有している一時鍵Ｋｔｅｍｐで復号し、暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを、伸張部６３と共有している一時鍵Ｋｔｅｍｐで再度、暗号化する。ステップＳ６８３において、SAM６

２は、伸張部６３と共有している一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを、伸張部６３に送信し、伸張部６３は、暗号化されたコンテンツ鍵Ｋｃｏを、受信する。

【０２８１】

ステップＳ６８４において、伸張部６３の復号モジュール７７は、受信部６１が受信したコンテンツ鍵Ｋｃｏを、SAM６２と共有する一時鍵Ｋｔｅｍｐで復号する。ステップＳ６８５において、伸張部６３の復号モジュール７６は、ステップＳ６７８で受信したコンテンツを、ステップＳ６８４で復号したコンテンツ鍵Ｋｃｏで復号する。ステップＳ６８６において、伸張部６３の伸張モジュール７８は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップＳ６８７において、ウォータマーク付加モジュール７９は、伸張されたコンテンツにレシーバ５１を特定する所定のウォータマークを挿入する。ステップＳ６８８において、伸張部６３は、図示せぬスピーカなどに再生されたコンテンツを出力する。ステップＳ６８９において、レシーバ５１のSAM６２は、メモリスティック１１１の通信部１３１に再生完了信号を送信し、メモリスティック１１１の制御ブロック１２１は、再生完了信号を受信し、処理は終了する。

【０２８２】

ステップＳ６７６において、ステップＳ６７５で算出したハッシュ値と、記憶部１３５に記憶されている、コンテンツIDに対応したコンテンツ鍵Ｋｃｏを記憶している鍵データブロックに対応する検査値とを比較し、一致しないと判定された場合、コンテンツ鍵Ｋｃｏなどに改竄があるので、処理は終了する。

【０２８３】

このように、鍵データブロックの改竄が無いときのみ、レシーバ５１に装着されているメモリスティック１１１に記憶されているコンテンツを、レシーバ５１は再生する。なお、ステップＳ６７１において、伸張部６３とメモリスティック１１１が、相互認証し、メモリスティック１１１は、コンテンツ鍵Ｋｃｏを伸張部６３に直接送信し、伸張部６３はコンテンツ鍵Ｋｃｏを受信するようにしてもよい。

【０２８４】

続いて、ユーザネットワーク５が図３０の構成を有し、暗号化されている検査値が記憶部１３５に記憶されているときの、レシーバ５１に装着されている鍵データ１４３に記憶されているコンテンツを、レシーバ５１が再生する処理を、図７４のフローチャートを参照して説明する。ステップＳ７０１乃至ステップＳ７０５の処理は、図７３のステップＳ６７１乃至ステップＳ６７５の処理とそれぞれ同様なので、その説明は省略する。

【０２８５】

ステップＳ７０６において、メモリスティック１１１の復号部１３６は、コンテンツ鍵Ｋｃｏを記憶している鍵データブロックに対応する検査値を記憶部１３５が記憶する検査用鍵Ｋｃｈで復号する。ステップＳ７０７において、データ検査部１３１は、ステップＳ７０５で得られたハッシュ値と、ステップＳ７０６で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップＳ７０８に進む。

【０２８６】

ステップＳ７０８乃至ステップＳ７２０の処理は、図７３のステップＳ６７７乃至ステップＳ６８９の処理とそれぞれ同様なので、その説明は省略する。

【０２８７】

ステップＳ７０７において、ステップＳ７０５で得られたハッシュ値と、ステップＳ７０６で復号された検査値とを比較し、一致しないと判定された場合、その鍵データブロックのデータは改竄されているので、処理は終了する。

【０２８８】

以上のように、暗号化されている検査値が記憶部１３５に記憶されているときも、鍵データブロックの改竄が無いときのみ、レシーバ５１に装着されているメモリスティック１１１に記憶されているコンテンツを、レシーバ５１は再生する。

【０２８９】

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動

画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればMPEG(Moving Picture Experts Group)などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

【０２９０】

また、共通鍵暗号は、ブロック暗号であるDESを使用して説明したが、NTT（商標）が提案するFEAL、IDEA(International Data Encription Algorithm)、または１ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

【０２９１】

さらに、コンテンツおよびコンテンツ鍵Ｋｃｏの暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

【０２９２】

また、図６５のステップＳ５１６、図６７のステップＳ５５７、図６９のステップＳ５９３、図７１のステップＳ６３３、図７３のステップＳ６７３、および図７４のステップＳ７０３において、レシーバ５１は、メモリスティック１１１に送信するコマンドに、レシーバ５１の秘密鍵で暗号化した署名を付して、メモリスティック１１１に送信し、メモリスティック１１１は、その署名を検査することにより、不正に対する耐性をより強化するようにしてもよい。

【０２９３】

さらに、図６５乃至図７２のコンテンツの移動の処理において、コンテンツ鍵Ｋｃｏは、再暗号化され、一時的に記憶された後、削除されるとして説明したが、コンテンツ鍵Ｋｃｏを受け取る側が、コンテンツ鍵を記憶する領域がない等の理由により、コンテンツ鍵Ｋｃｏを削除し、コンテンツ鍵Ｋｃｏを受け取れなかった場合の不都合を回避する為に、コンテンツ鍵Ｋｃｏを送る側は、受信完了信号を受信するまで、コンテンツ鍵Ｋｃｏを一時的に使用不可（コンテンツ鍵Ｋｃｏの状態を示すフラグを定義し、そのフラグを使用する等の処理をする）とし、受信完了信号を受信できなかったときは、そのコンテンツ鍵Ｋｃｏを再度、使用できるような処理を行っても良い。

【０２９４】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【０２９５】

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【０２９６】

【発明の効果】

請求項１に記載の情報処理装置、請求項３に記載の情報処理方法、および請求項４に記載の提供媒体によれば、情報の使用の許諾条件を示す情報を生成し、許諾条件を示す情報の認証情報を生成し、認証情報を記憶するようにしたので、情報の使用の許諾条件の書き換えを検出し、対応することができる。

【０２９７】

請求項５に記載の情報処理装置、請求項９に記載の情報処理方法、および請求項１０に記載の提供媒体によれば、情報の利用のときに必要な関連情報の認証情報を生成し、認証情報を記憶し、関連情報から、他の認証情報を生成し、記憶している認証情報との一致を検証し、情報記憶媒体と相互認証するようにしたので、情報の関連情報の書き換えを検出し、対応することができる。

【０２９８】

請求項１１に記載の情報記憶媒体によれば、認証情報生成手段が、情報の利用のときに必要な関連情報の認証情報を生成し、記憶手段認が証情報を記憶し、検証手段が、関連情報から、他の認証情報を生成し、記憶手段が記憶している認証情報との一致を検証し、相互認証手段が、情報処理装置と相互認証するようにしたので、情報の関連情報の書き換えを検出し、対応することができる。

【図面の簡単な説明】

【図１】

EMDのシステムを説明する図である。

【図２】

EMDサービスセンタ１の機能の構成を示すブロック図である。

【図３】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図４】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図５】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図６】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図７】

ユーザ登録データベースを説明する図である。

【図８】

コンテンツプロバイダ２の機能の構成を示すブロック図である。

【図９】

サービスプロバイダ３の機能の構成を示すブロック図である。

【図１０】

ユーザホームネットワーク５の構成を示すブロック図である。

【図１１】

ユーザホームネットワーク５の構成を示すブロック図である。

【図１２】

コンテンツおよびコンテンツに付随する情報を説明する図である。

【図１３】

コンテンツプロバイダセキュアコンテナを説明する図である。

【図１４】

コンテンツプロバイダ２の証明書を説明する図である。

【図１５】

サービスプロバイダセキュアコンテナを説明する図である。

【図１６】

サービスプロバイダ３の証明書を説明する図である。

【図１７】

取扱方針、価格情報、および使用許諾条件情報を示す図である。

【図１８】

シングルコピーおよびマルチコピーを説明する図である。

【図１９】

取扱方針および価格情報を説明する図である。

【図２０】

取扱方針、価格情報、および使用許諾条件情報を説明する図である。

【図２１】

コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図２２】

サービスプロバイダセキュアコンテナを説明する図である。

【図２３】

取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。

【図２４】

コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図２５】

コンテンツプロバイダセキュアコンテナを説明する図である。

【図２６】

サービスプロバイダセキュアコンテナを説明する図である。

【図２７】

EMDサービスセンタ１の、ユーザホームネットワーク５からの課金情報の受信のときの動作を説明する図である。

【図２８】

EMDサービスセンタ１の利益分配処理の動作を説明する図である。

【図２９】

EMDサービスセンタ１の、コンテンツの利用実績の情報をJASRACに送信する処理の動作を説明する図である。

【図３０】

ユーザホームネットワーク５の更に他の実施の形態の構成を示す図である。

【図３１】

外部記憶部１１３の記憶の態様を説明する図である。

【図３２】

記憶モジュール７３の記憶の態様を説明する図である。

【図３３】

外部記憶部１１３の他の記憶の態様を説明する図である。

【図３４】

記憶モジュール７３の他の記憶の態様を説明する図である。

【図３５】

鍵データ１４３の記憶の態様を説明する図である。

【図３６】

記憶部１３５の記憶の態様を説明する図である。

【図３７】

鍵データ１４３の他の記憶の態様を説明する図である。

【図３８】

記憶部１３５の他の記憶の態様を説明する図である。

【図３９】

コンテンツの配布の処理を説明するフローチャートである。

【図４０】

コンテンツの配布の処理を説明するフローチャートである。

【図４１】

EMDサービスセンタ１がコンテンツプロバイダ２へ配送用鍵Ｋｄを送信する処理を説明するフローチャートである。

【図４２】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図４３】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図４４】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図４５】

レシーバ５１のEMDサービスセンタ１への登録の処理を説明するフローチャートである。

【図４６】

SAMの証明書を説明する図である。

【図４７】

登録リストを説明する図である。

【図４８】

ICカード５５へのSAM６２のデータのバックアップの処理を説明するフローチャートである。

【図４９】

ICカード５５へのSAM６２のデータのバックアップの処理を説明するフローチャートである。

【図５０】

新しいレシーバにICカード５５のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図５１】

新しいレシーバにICカード５５のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図５２】

レシーバ５１が、従属関係のあるレコーダ５３をEMDサービスセンタ１に登録する処理を説明するフローチャートである。

【図５３】

レシーバ５１がEMDサービスセンタ１から配送用鍵Ｋｄを受け取る処理を説明するフローチャートである。

【図５４】

レコーダの配送用鍵Ｋｄの受け取り処理を説明するフローチャートである。

【図５５】

コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図５６】

コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する他の処理を説明するフローチャートである。

【図５７】

サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図５８】

サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図５９】

レシーバ５１の課金処理を説明するフローチャートである。

【図６０】

レシーバ５１の適正なサービスプロバイダセキュアコンテナを受信し、課金する処理の詳細を説明するフローチャートである。

【図６１】

レシーバ５１の適正なサービスプロバイダセキュアコンテナを受信し、課金する処理の詳細を説明するフローチャートである。

【図６２】

MDドライブ５４から供給される暗号化されていないコンテンツを、暗号化し、記録する処理の詳細を説明するフローチャートである。

【図６３】

レシーバ５１がコンテンツを再生する処理を説明するフローチャートである。

【図６４】

レシーバ５１がデコーダ５６にコンテンツを再生させる処理を説明するフローチャートである。

【図６５】

レシーバ５１からメモリスティック１１１にコンテンツを移動する処理を説明するフローチャートである。

【図６６】

レシーバ５１からメモリスティック１１１にコンテンツを移動する処理を説明するフローチャートである。

【図６７】

レシーバ５１からメモリスティック１１１にコンテンツを移動するフローチャートである。

【図６８】

レシーバ５１からメモリスティック１１１にコンテンツを移動するフローチャートである。

【図６９】

メモリスティック１１１からレシーバ５１にコンテンツを移動するフローチャートである。

【図７０】

メモリスティック１１１からレシーバ５１にコンテンツを移動するフローチャートである。

【図７１】

メモリスティック１１１からレシーバ５１にコンテンツを移動する処理を説明するフローチャートである。

【図７２】

メモリスティック１１１からレシーバ５１にコンテンツを移動する処理を説明するフローチャートである。

【図７３】

メモリスティック１１１に記憶されているコンテンツをレシーバ５１が再生する処理を説明するフローチャートである。

【図７４】

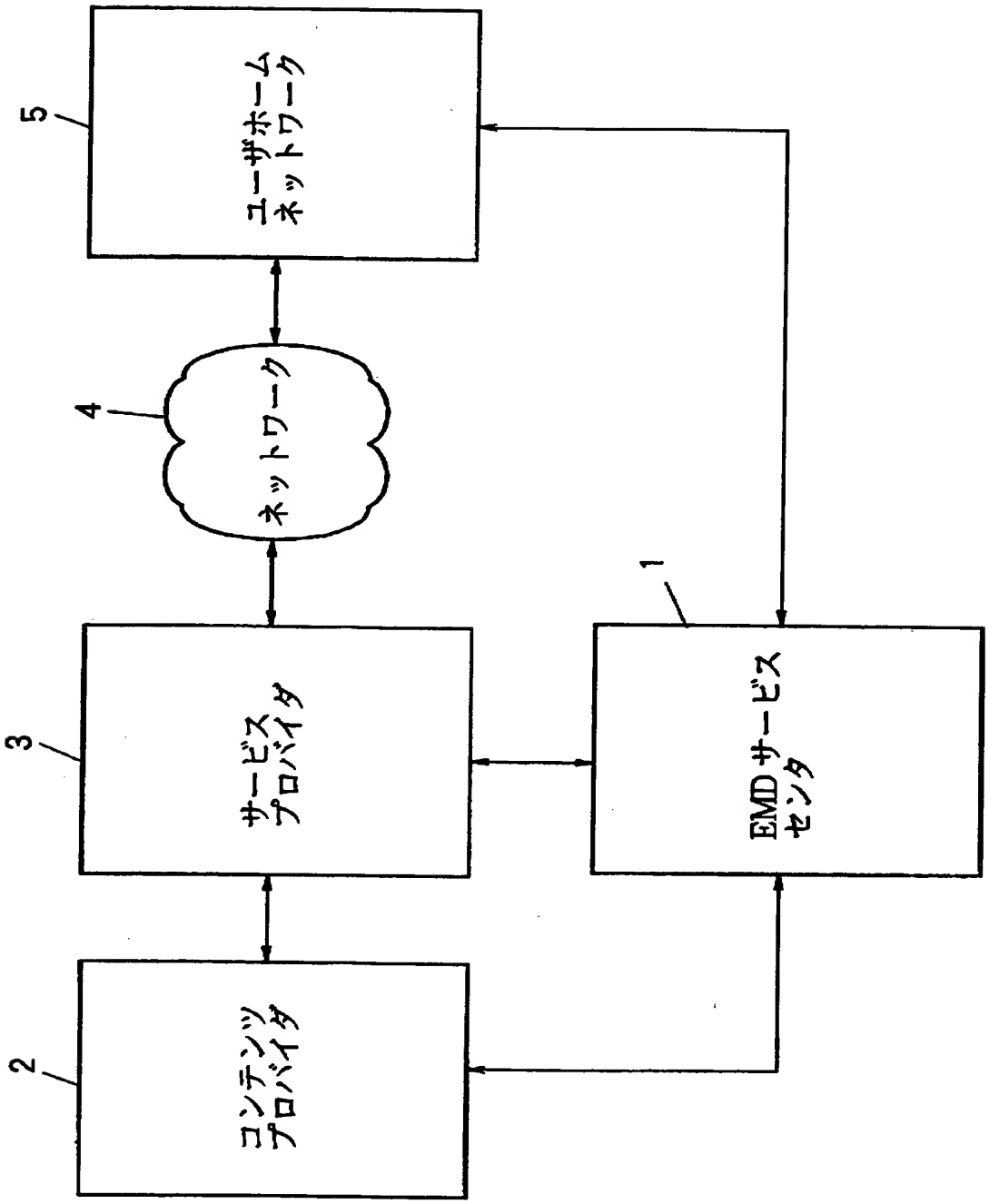
メモリスティック１１１に記憶されているコンテンツをレシーバ５１が再生する処理を説明するフローチャートである。

【符号の説明】

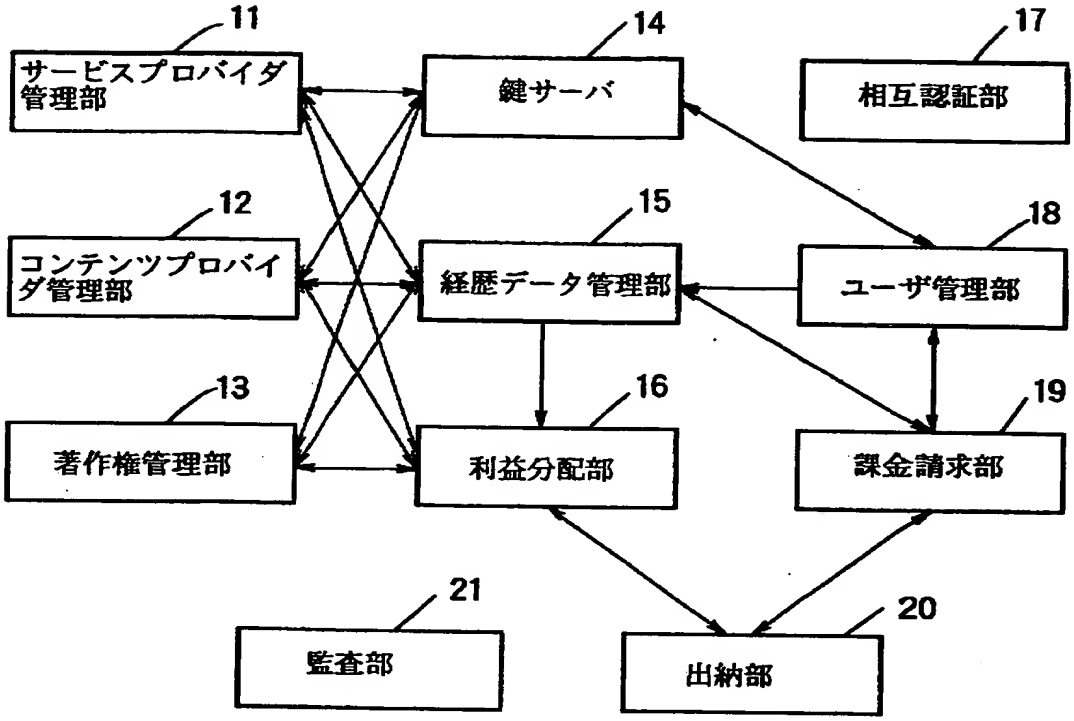
１　EMDサービスセンタ，　２　コンテンツプロバイダ、　３　サービスプロバイダ，５　ユーザホームネットワーク，　１６　利益分配部，　１８　ユーザ管理部，　４２　値付け部，　５１　レシーバ，　５６　デコーダ，　６１　通信部，　６２　SAM，　６３　伸張部，　７１　相互認証モジュール，　７２　課金処理モジュール，　７３　記憶モジュール，　７４　復号／暗号化モジュール，　７５　相互認証モジュール，　７６　復号モジュール，　７７　復号モジュール，　８１　相互認証モジュール，　９１　復号ユニット，　９２　乱数発生ユニット，　９３　暗号化ユニット，　１０１　相互認証モジュール，　１０２　復号モジュール，　１０３　復号モジュール，　１１３　外部記憶部，　１１４　データ検査モジュール，　１２１　制御ブロック，　１２２　情報記憶ブロック，　１３１　通信部，　１３２　メモリコントローラ，　１３３　相互認証部，　１３４　暗号化部，　１３５　記憶部，　１３６　復号部，　１３７　乱数生成部，　１３８　データ検査部，　１４３　鍵データ，　１４４　暗号化データ

【書類名】　図面

【図１】

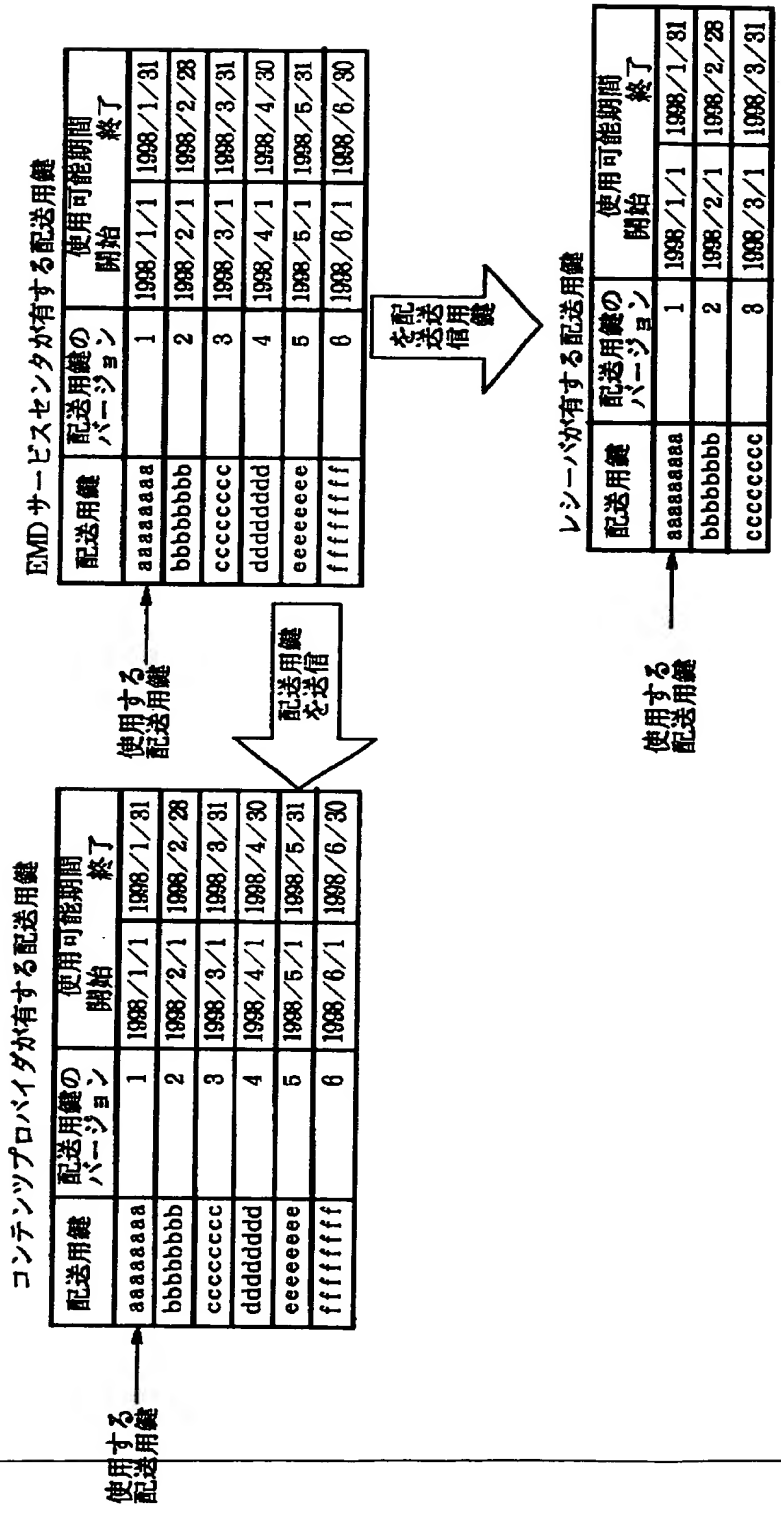

5
ユーザホーム
ネットワーク
4
ネットワーク
1
3
サービス
プロバイダ
EMD サービス
センタ
2
コンテンツ
プロバイダ

【図２】

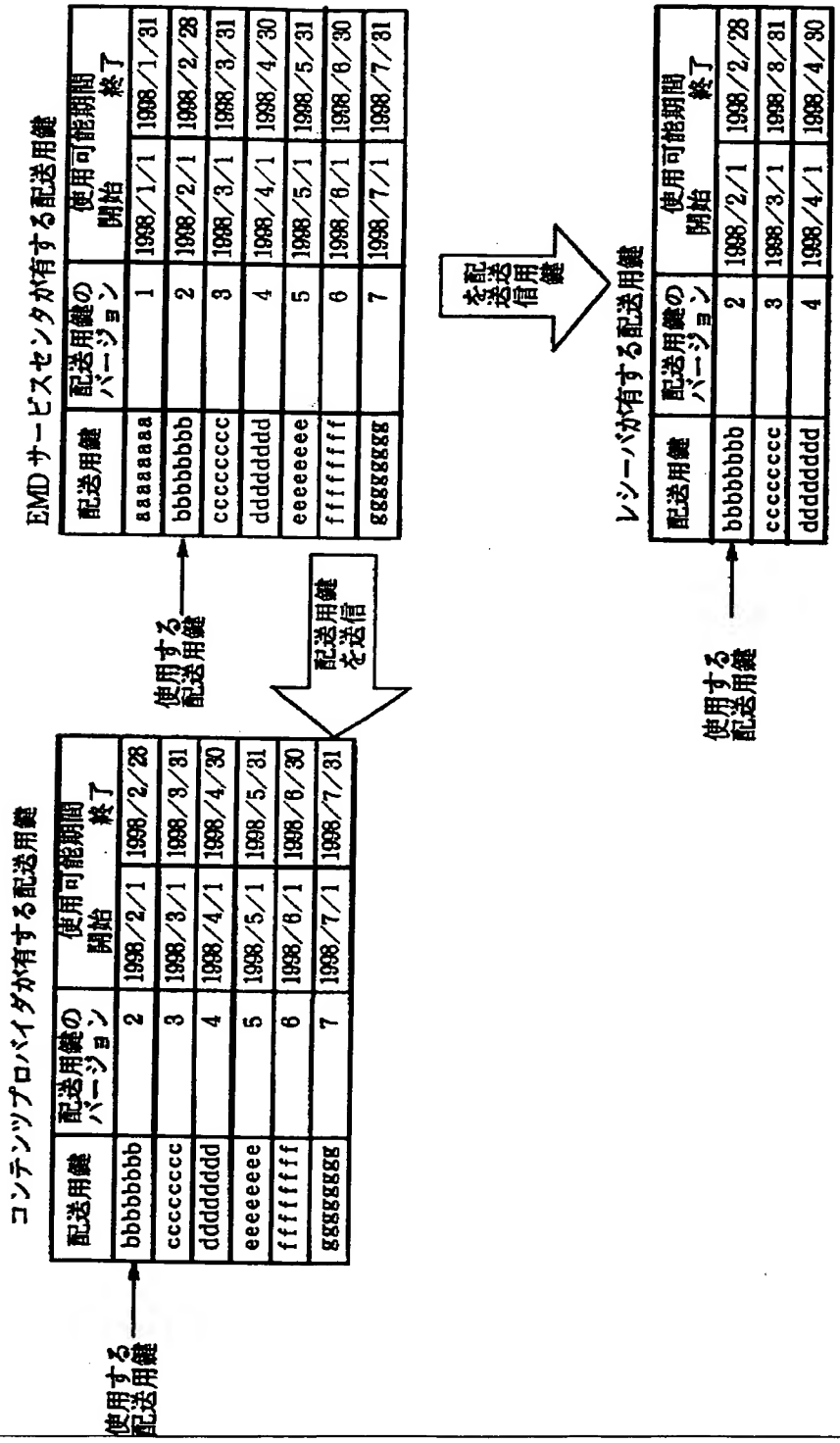


EMD サービスセンタ 1

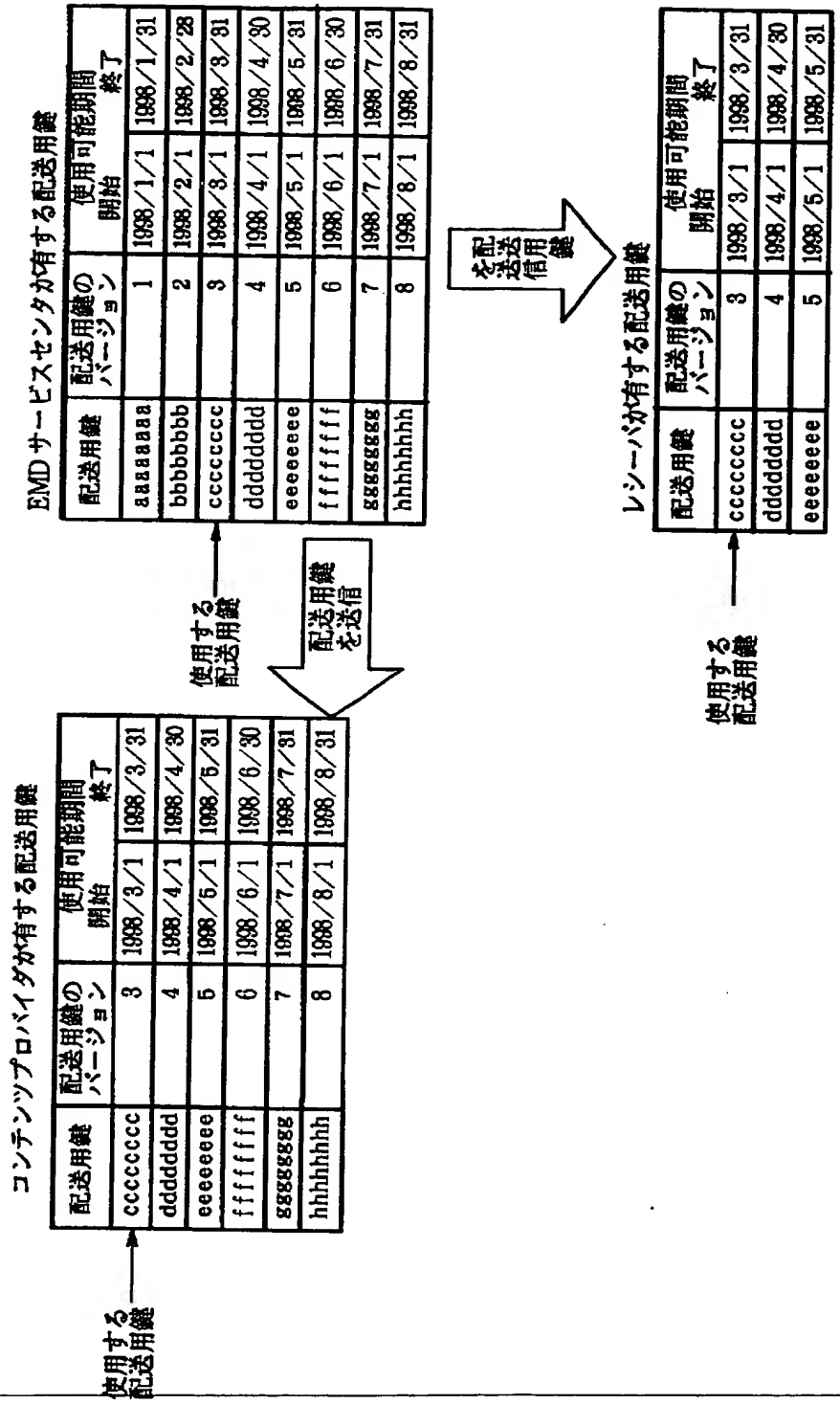
【図３】


コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
配送用鍵を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
使用する配送用鍵

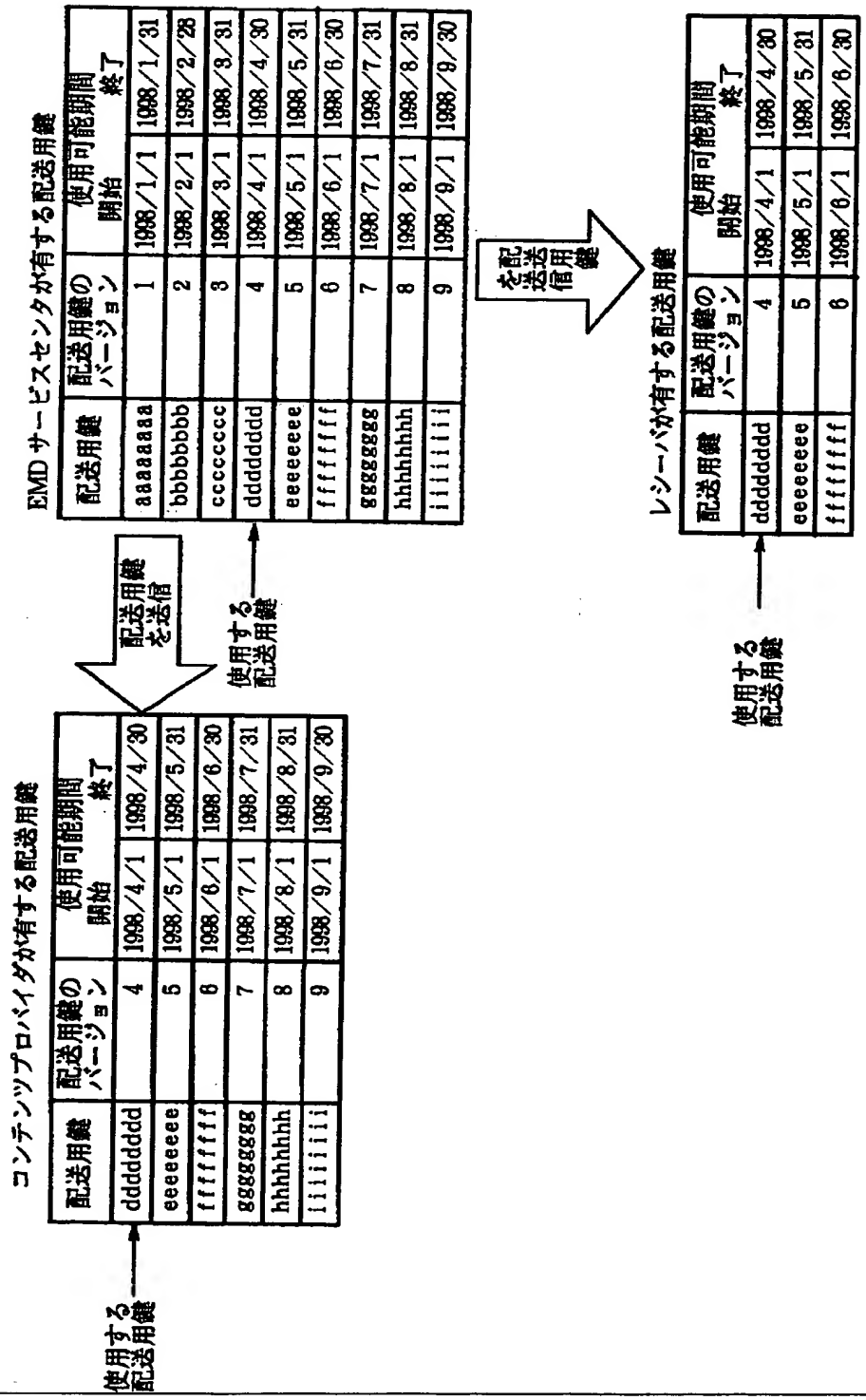
【図４】


EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
使用する配送用鍵
配送用鍵を送信
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
使用する配送用鍵
配送用鍵を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
使用する配送用鍵

【図５】


EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
使用する配送用鍵
配送用鍵を送信
を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
使用する配送用鍵
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
使用する配送用鍵

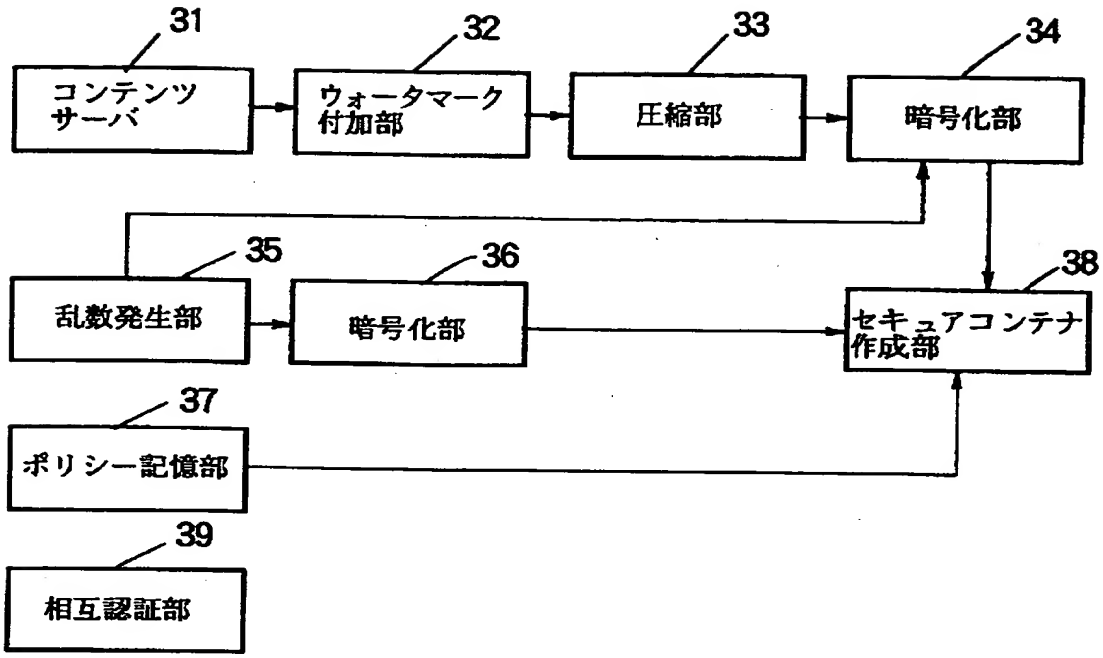
【図６】


EMD サービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiii 9 1998/9/1 1998/9/30
配送用鍵を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
配送用鍵を送信
使用する配送用鍵
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiii 9 1998/9/1 1998/9/30
使用する配送用鍵

【図７】

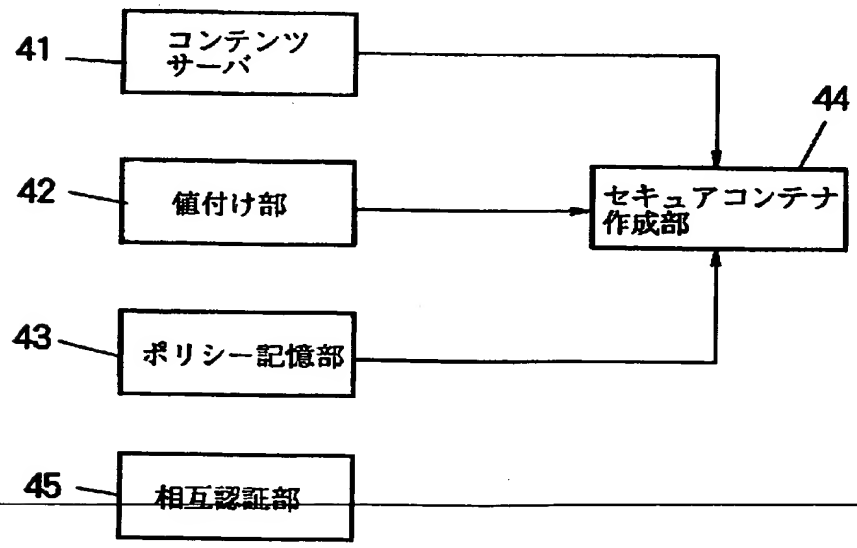
ID	決済処理	登録	EMDサービスセンタとの接続
0000000000000001h	可	可	可
0000000000000002h	可	可	不可
0000000000000003h	可	不可	可
0000000000000004h	可	不可	不可
0000000000000005h	不可	可	可
0000000000000006h	不可	可	不可
0000000000000007h	不可	不可	可
0000000000000008h	不可	不可	不可
0000000000000009h	可	可	可
・・・			
FFFFFFFFFFFFFFFEh	可	不可	不可
FFFFFFFFFFFFFFFFh	不可	可	可

【図８】



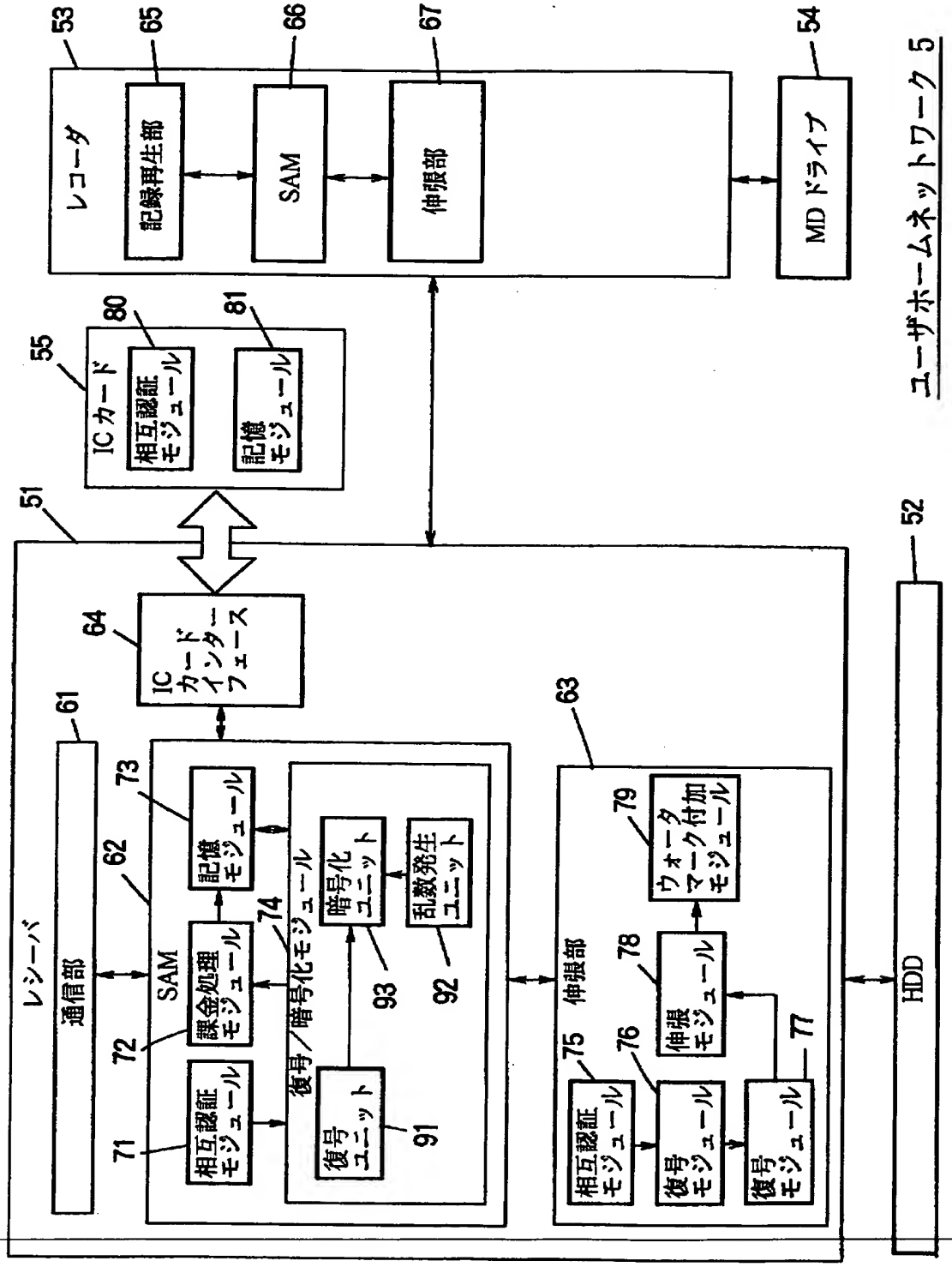
コンテンツプロバイダ 2

【図９】

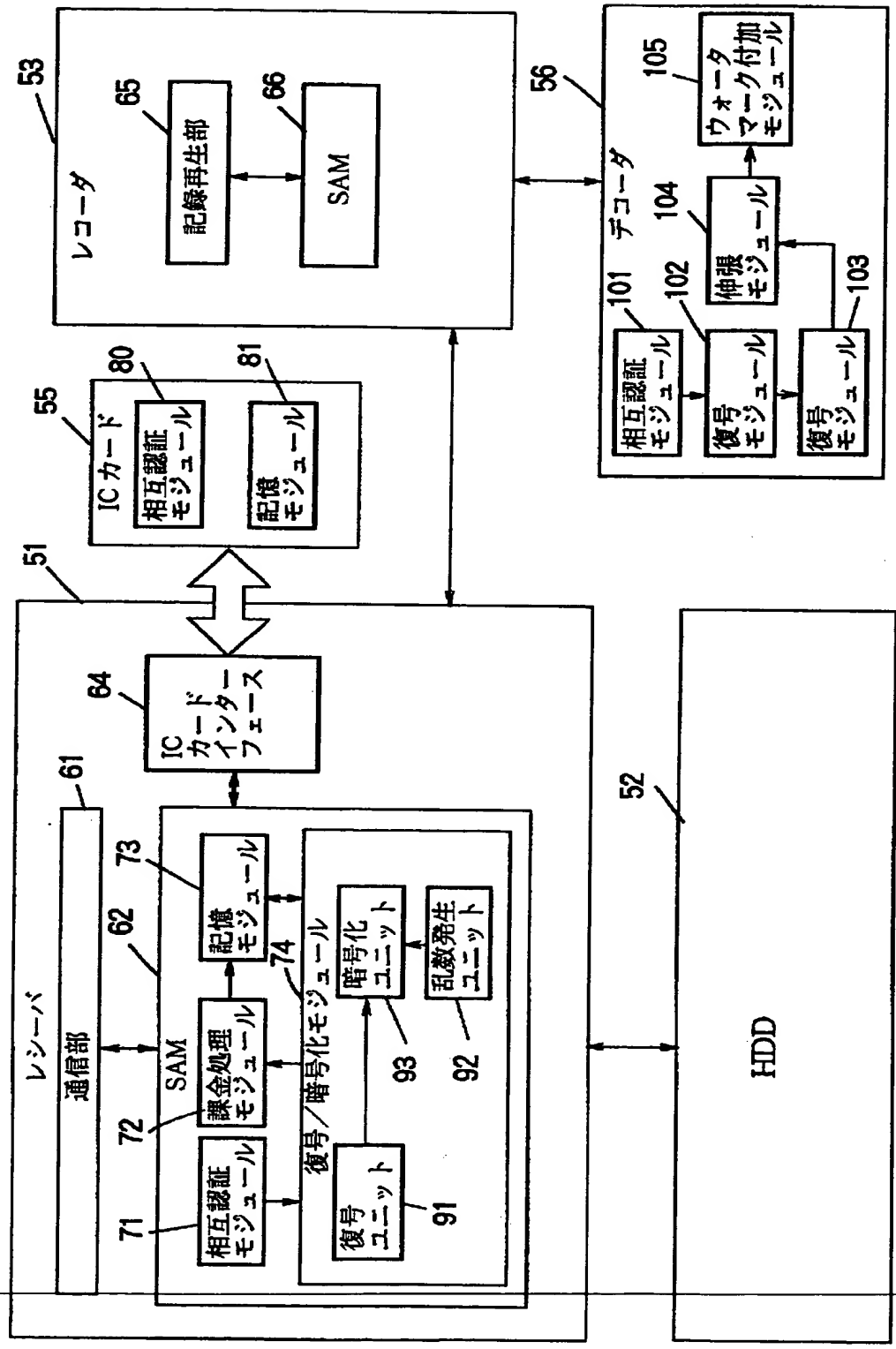


サービスプロバイダ 3

【図１０】

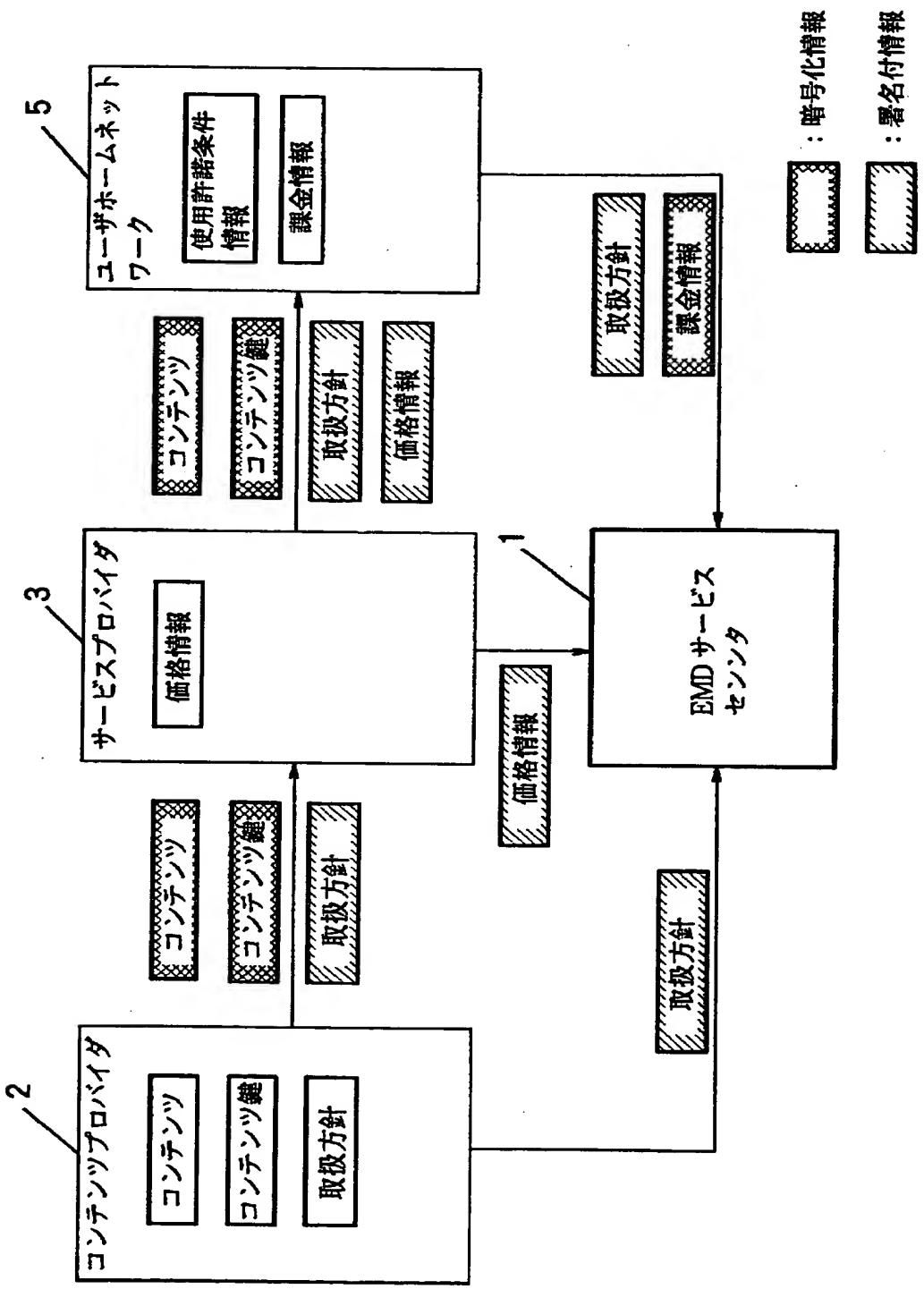

ユーザホームネットワーク 5
レコーダ
記録再生部
SAM
伸張部
MD ドライブ
ICカード
相互認証モジュール
記憶モジュール
ICカードインターフェース
レシーバ
通信部
SAM
記憶モジュール
課金処理モジュール
相互認証モジュール
復号／暗号化モジュール
暗号化ユニット
乱数発生ユニット
復号ユニット
伸張部
ウォータマーク付加モジュール
伸張モジュール
相互認証モジュール
復号モジュール
復号モジュール
HDD
51
52
53
54
55
61
62
63
64
65
66
67
71
72
73
74
75
76
77
78
79
80
81
91
92
93

【図１１】

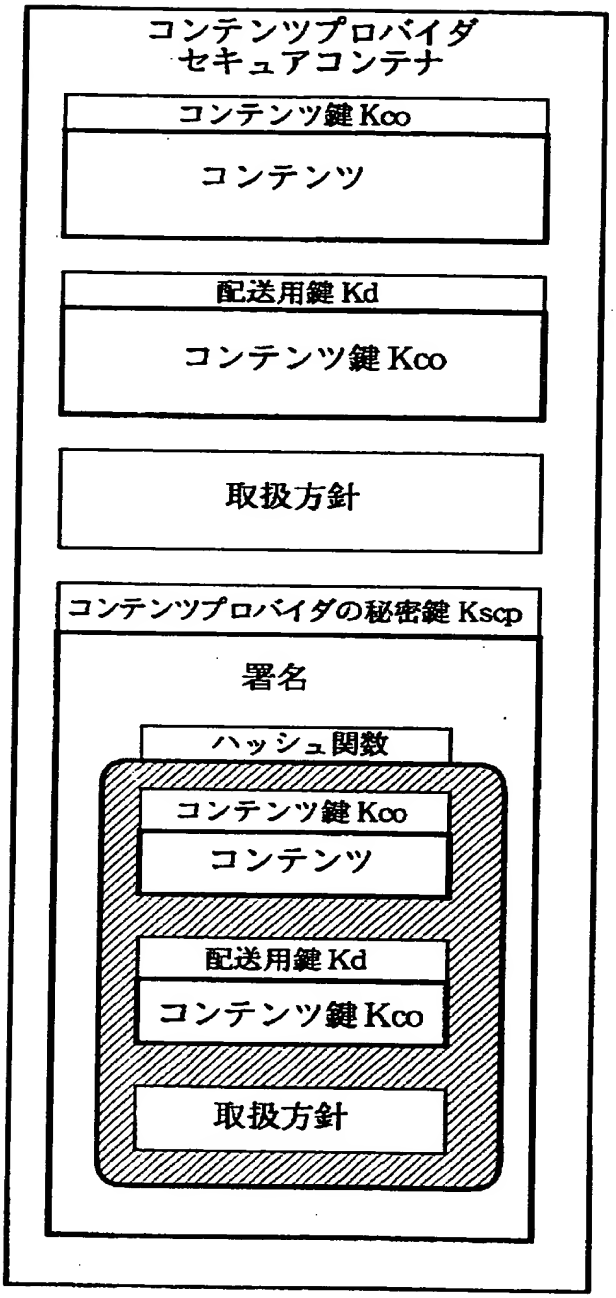


ユーザホームネットワーク５

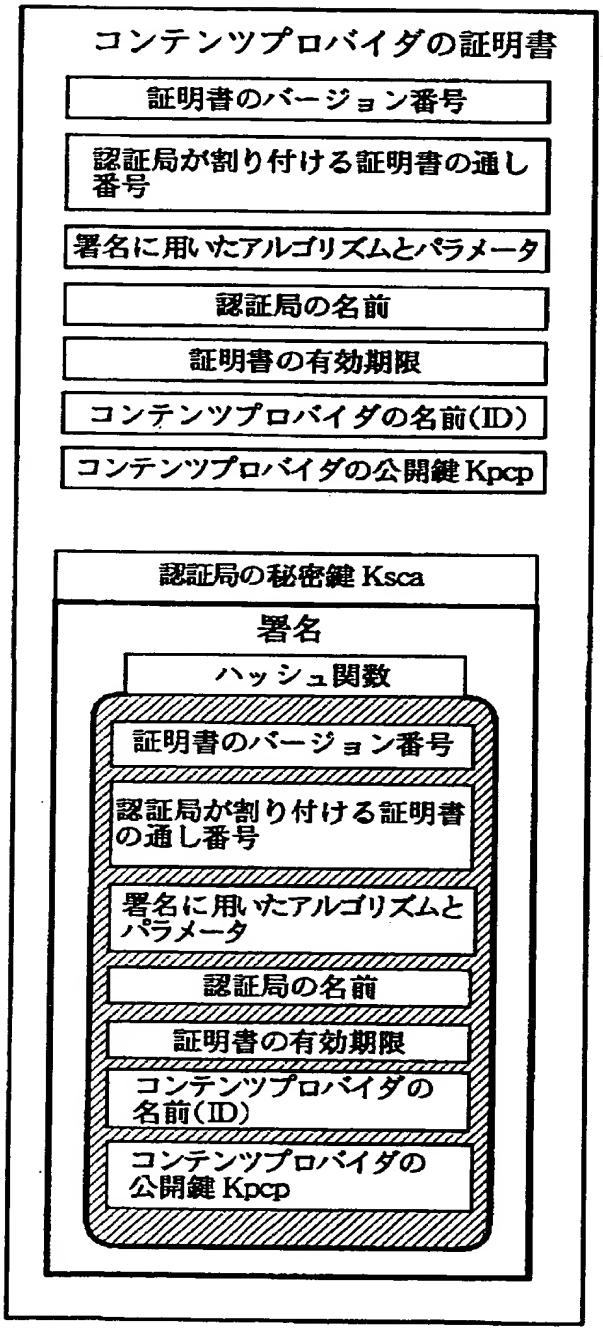
【図１２】


：暗号化情報
：署名付情報
5
ユーザホームネットワーク
使用許諾条件情報
課金情報
コンテンツ
コンテンツ鍵
取扱方針
価格情報
取扱方針
課金情報
3
サービスプロバイダ
価格情報
1
EMDサービスセンタ
価格情報
コンテンツ
コンテンツ鍵
取扱方針
取扱方針
2
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
取扱方針

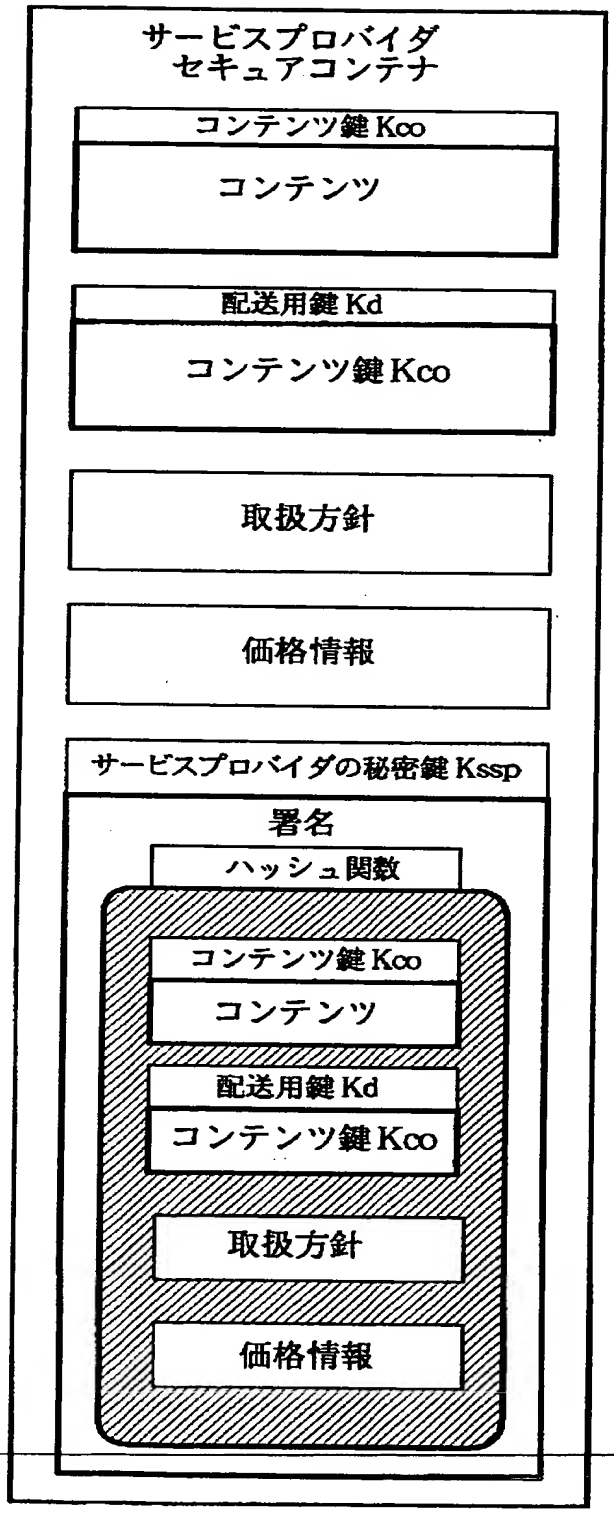
【図１３】


コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針
コンテンツプロバイダの秘密鍵 Kscp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針

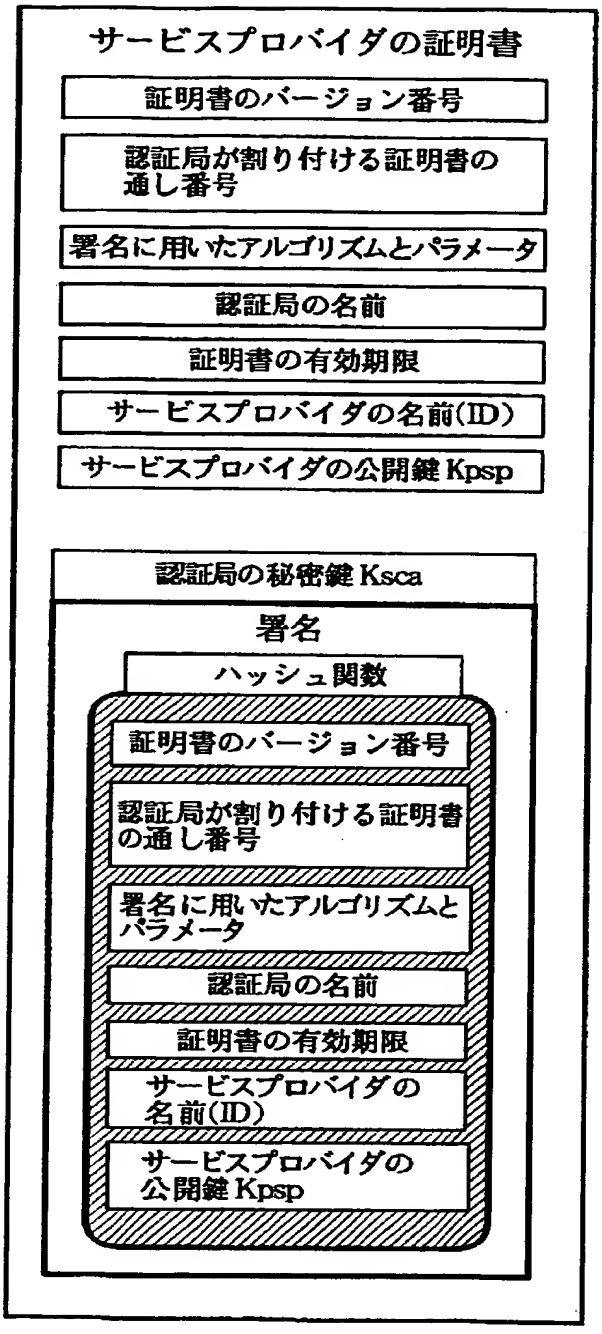
【図１４】


コンテンツプロバイダの証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
コンテンツプロバイダの名前(ID)
コンテンツプロバイダの公開鍵 Kpcp
認証局の秘密鍵 Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
コンテンツプロバイダの名前(ID)
コンテンツプロバイダの公開鍵 Kpcp

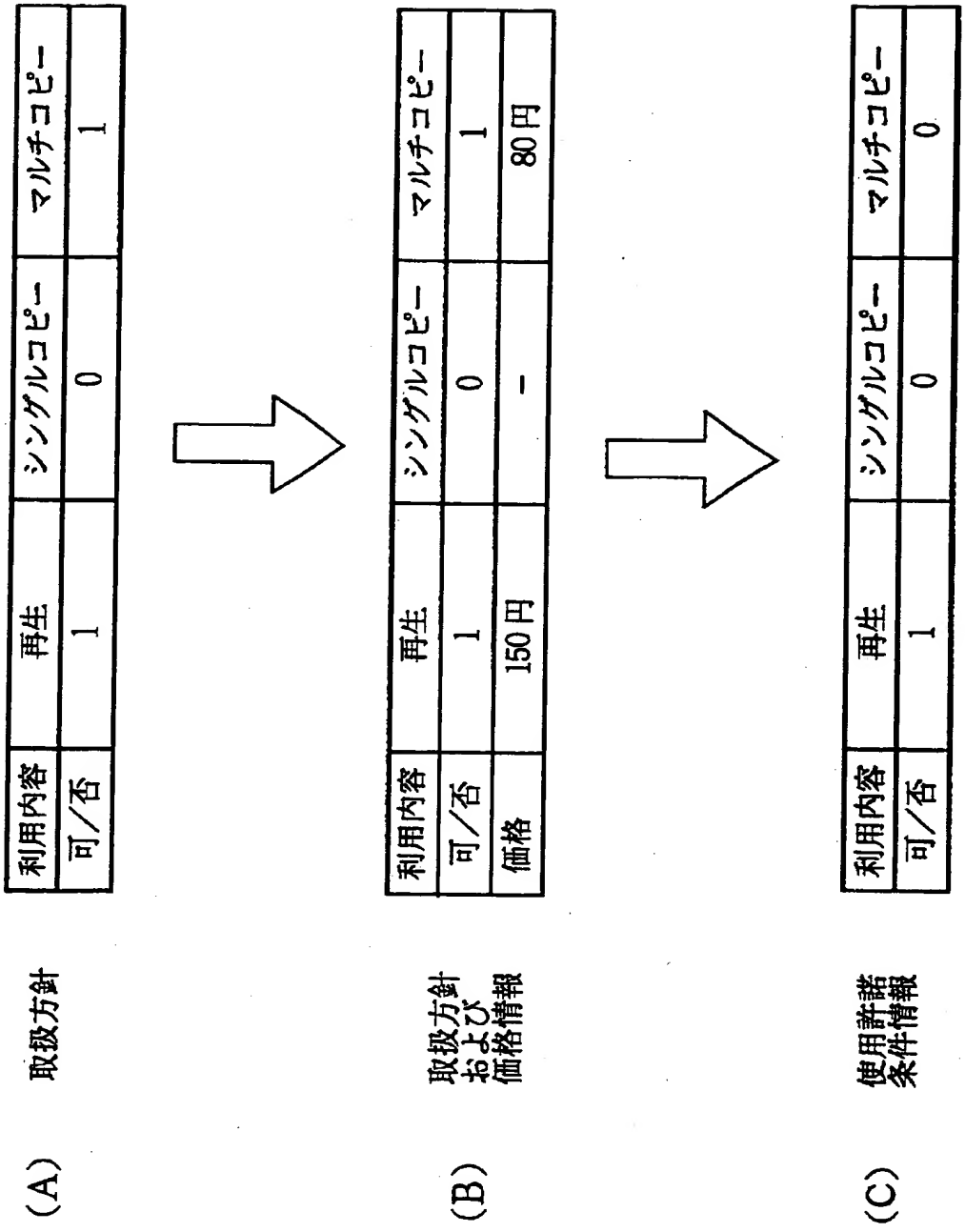
【図１５】


サービスプロバイダ
セキュアコンテナ
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針
価格情報
サービスプロバイダの秘密鍵 Kssp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
取扱方針
価格情報

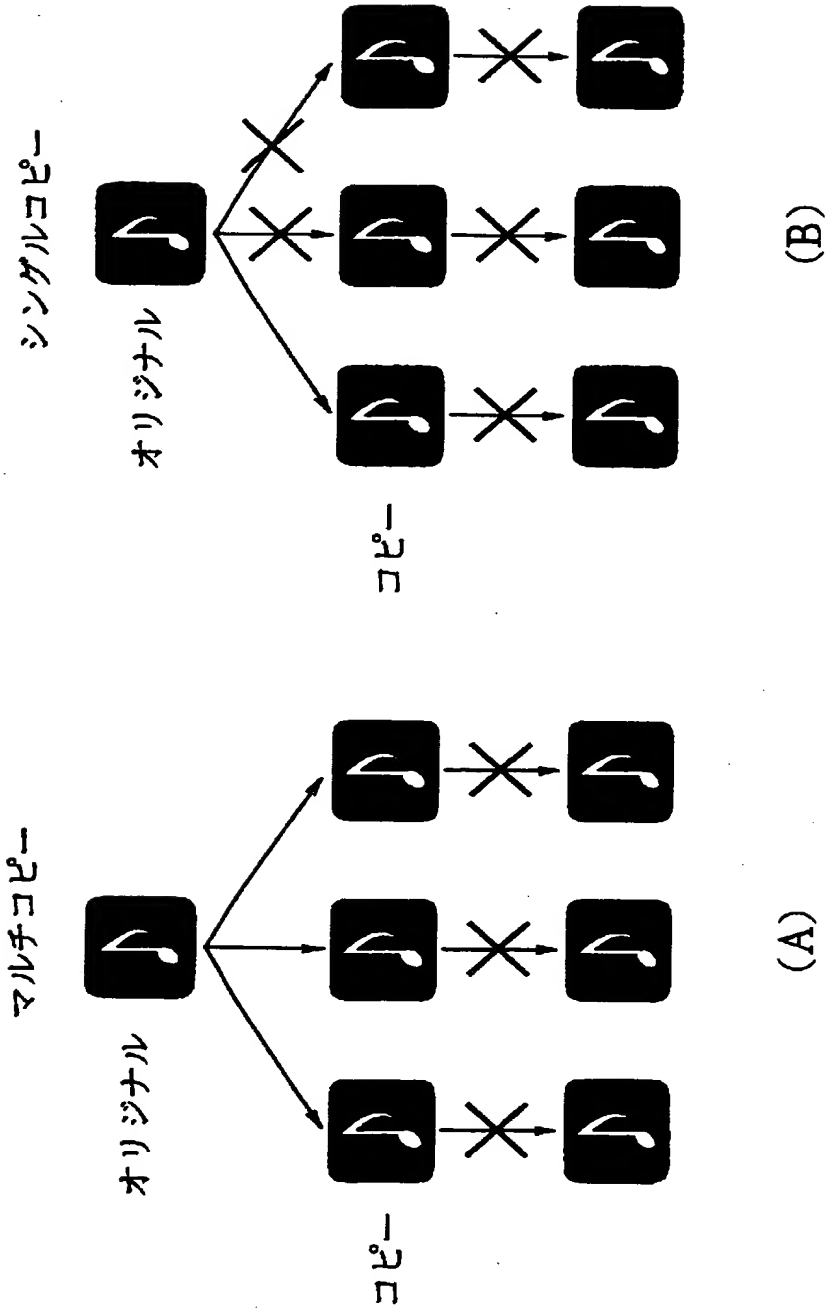
【図１６】


サービスプロバイダの証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
サービスプロバイダの名前(ID)
サービスプロバイダの公開鍵 Kpsp
認証局の秘密鍵 Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
サービスプロバイダの名前(ID)
サービスプロバイダの公開鍵 Kpsp

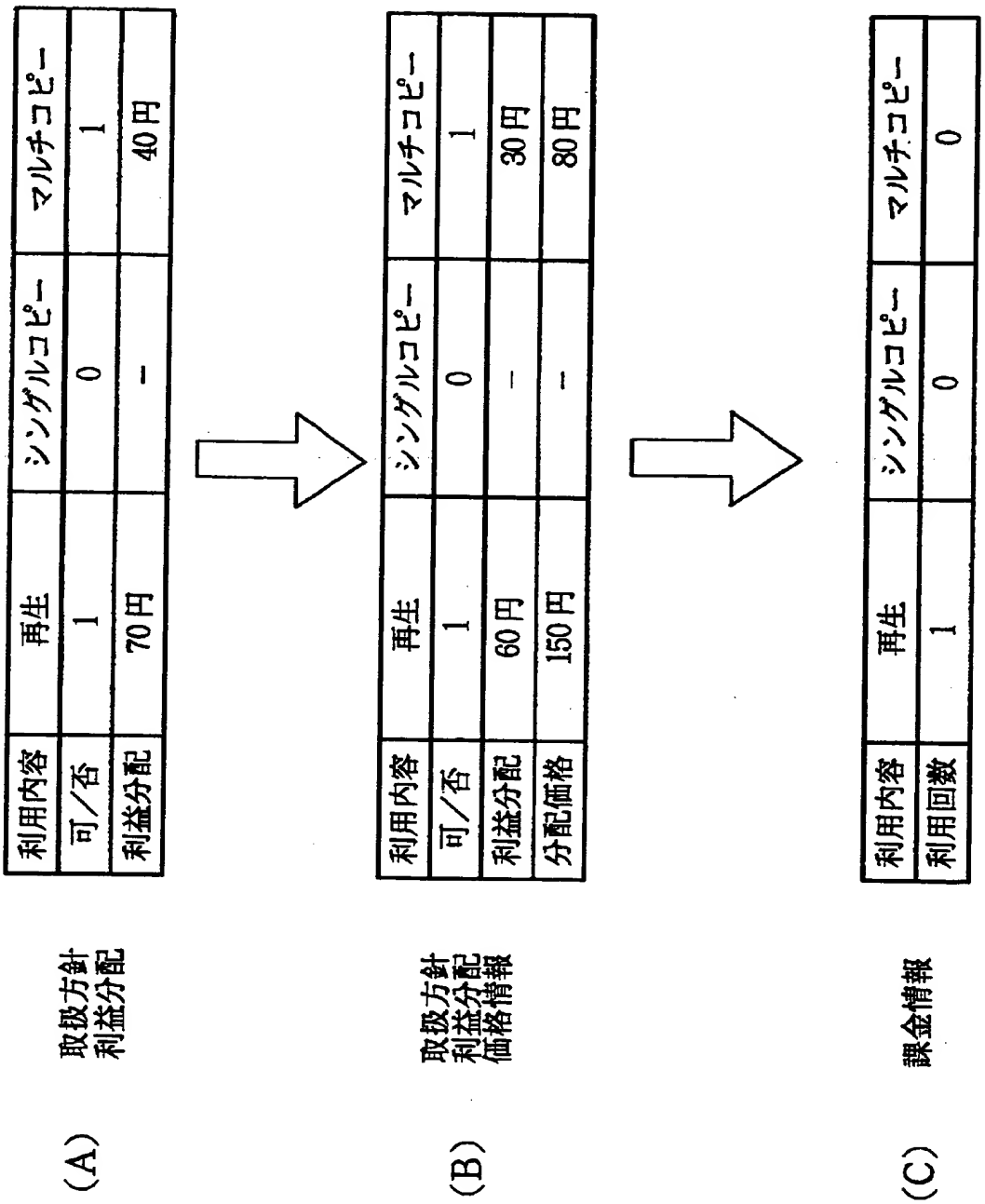
【図１７】


(A)
取扱方針
利用内容
再生
シングルコピー
マルチコピー
可／否
1
0
1
(B)
取扱方針
および
価格情報
利用内容
再生
シングルコピー
マルチコピー
可／否
1
0
1
価格
150円
－
80円
(C)
使用許諾
条件情報
利用内容
再生
シングルコピー
マルチコピー
可／否
1
0
0

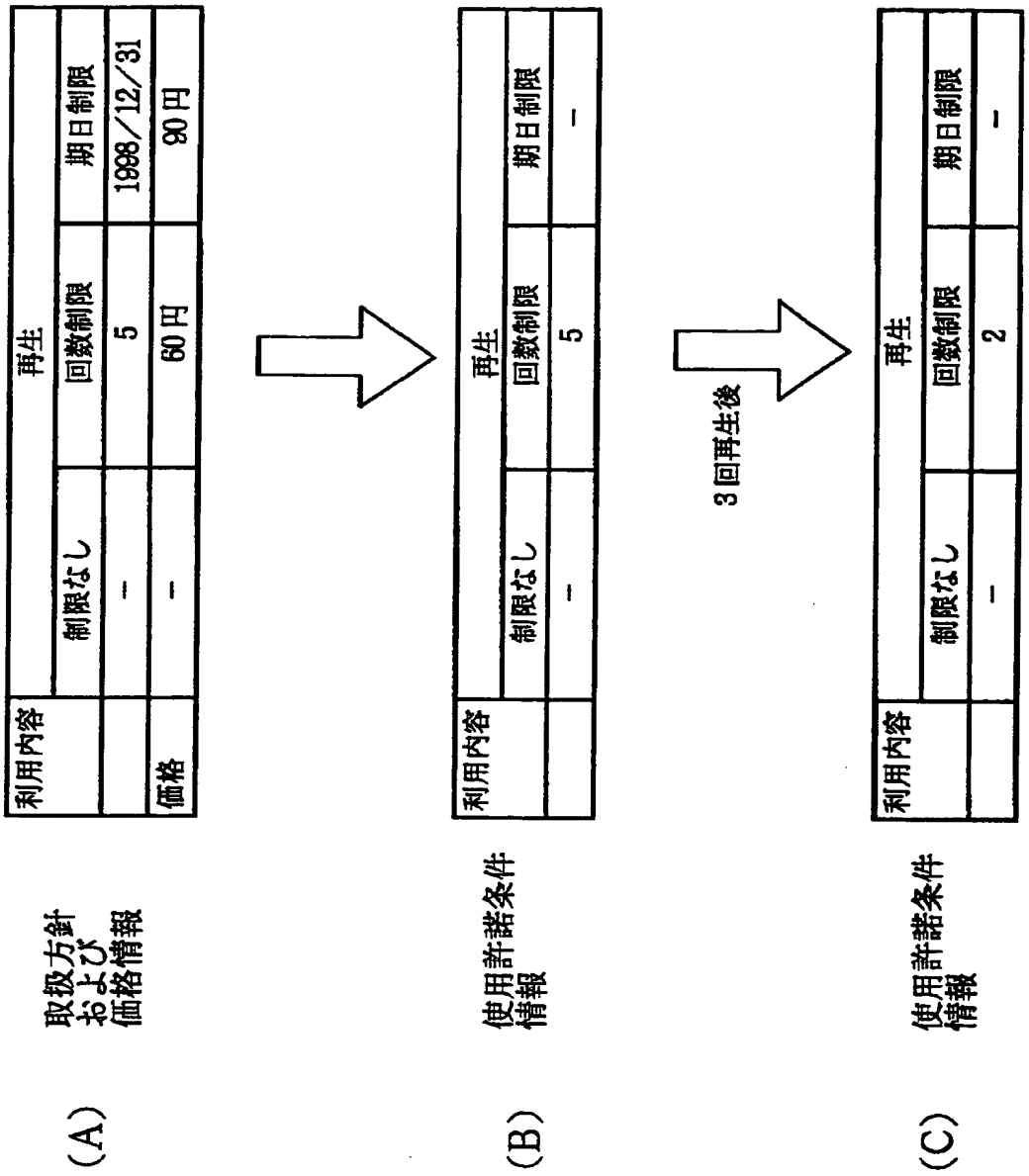
【図１８】



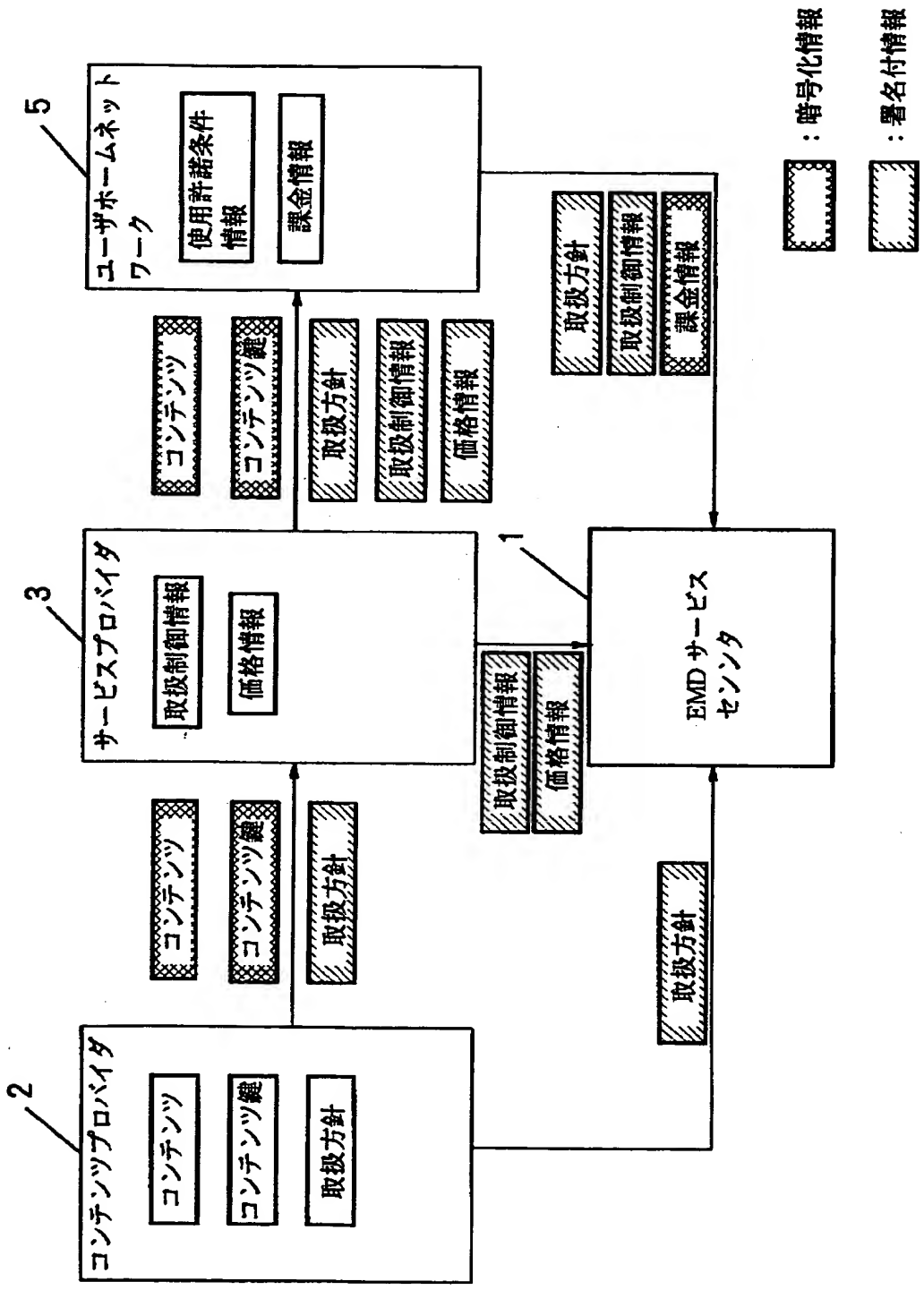
【図１９】


(A)
取扱方針
利益分配
利用内容
可／否
利益分配
再生
1
70円
シングルコピー
0
−
マルチコピー
1
40円
(B)
取扱方針
利益分配
価格情報
利用内容
可／否
利益分配
分配価格
再生
1
60円
150円
シングルコピー
0
−
−
マルチコピー
1
30円
80円
(C)
課金情報
利用内容
利用回数
再生
1
シングルコピー
0
マルチコピー
0

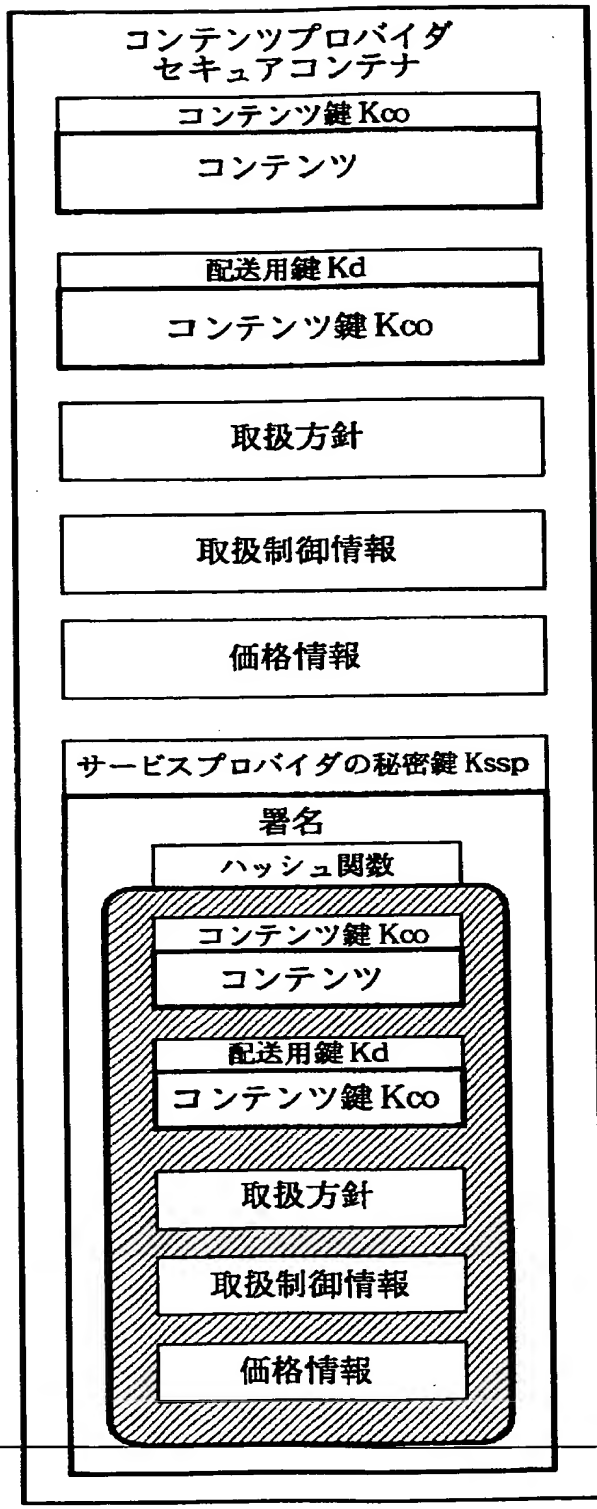
【図２０】


(A)
取扱方針および価格情報
利用内容
再生
制限なし
回数制限
期日制限
－
5
1998／12／31
価格
－
60円
90円
(B)
使用許諾条件情報
利用内容
再生
制限なし
回数制限
期日制限
－
5
－
3回再生後
(C)
使用許諾条件情報
利用内容
再生
制限なし
回数制限
期日制限
－
2
－

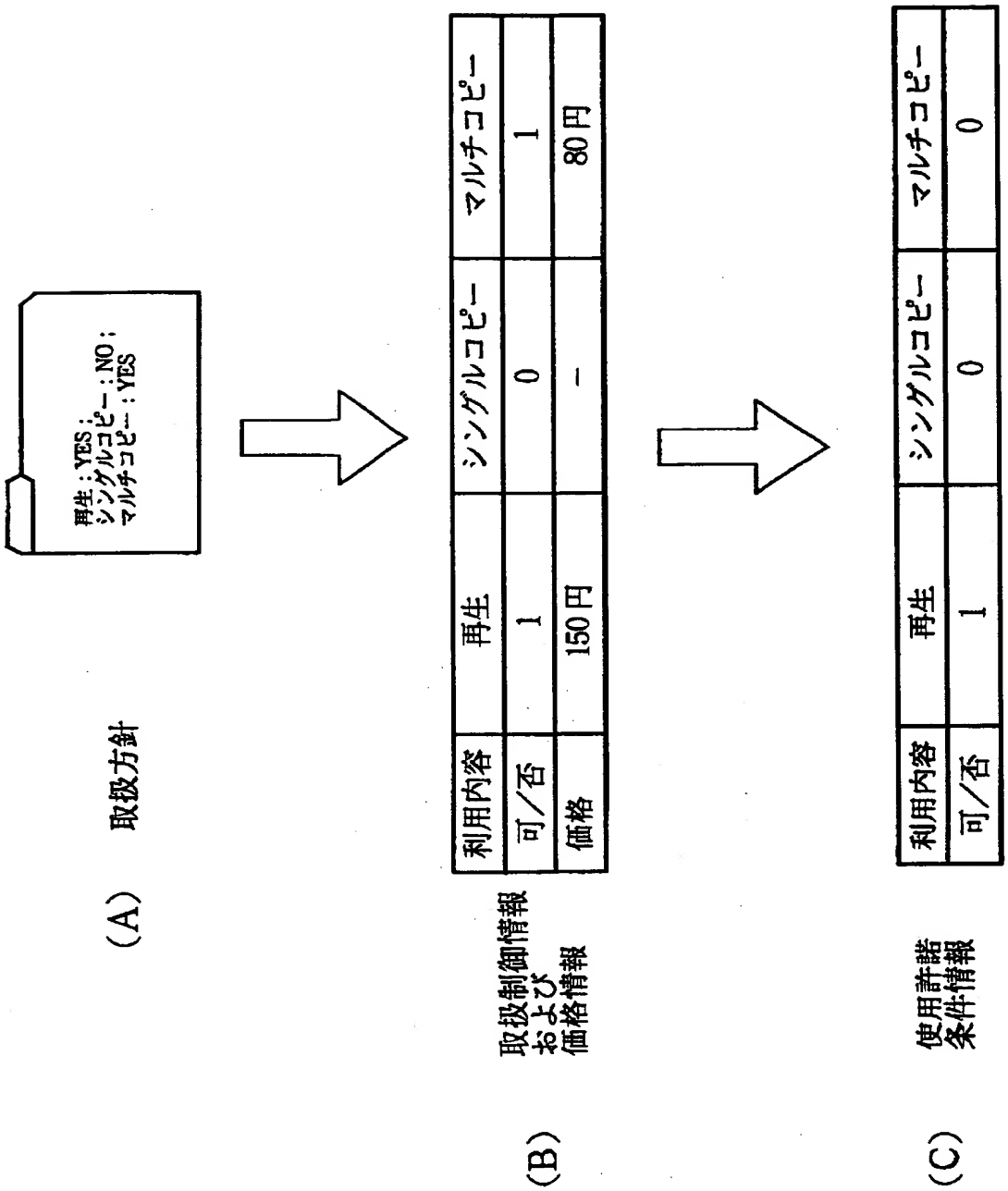
【図２１】


：暗号化情報
：署名付情報
5
ユーザホームネットワーク
使用許諾条件情報
課金情報
3
サービスプロバイダ
取扱制御情報
価格情報
2
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
取扱方針
1
EMDサービスセンタ
コンテンツ
コンテンツ鍵
取扱方針
取扱制御情報
価格情報
取扱方針
取扱制御情報
課金情報
取扱方針
取扱制御情報
価格情報

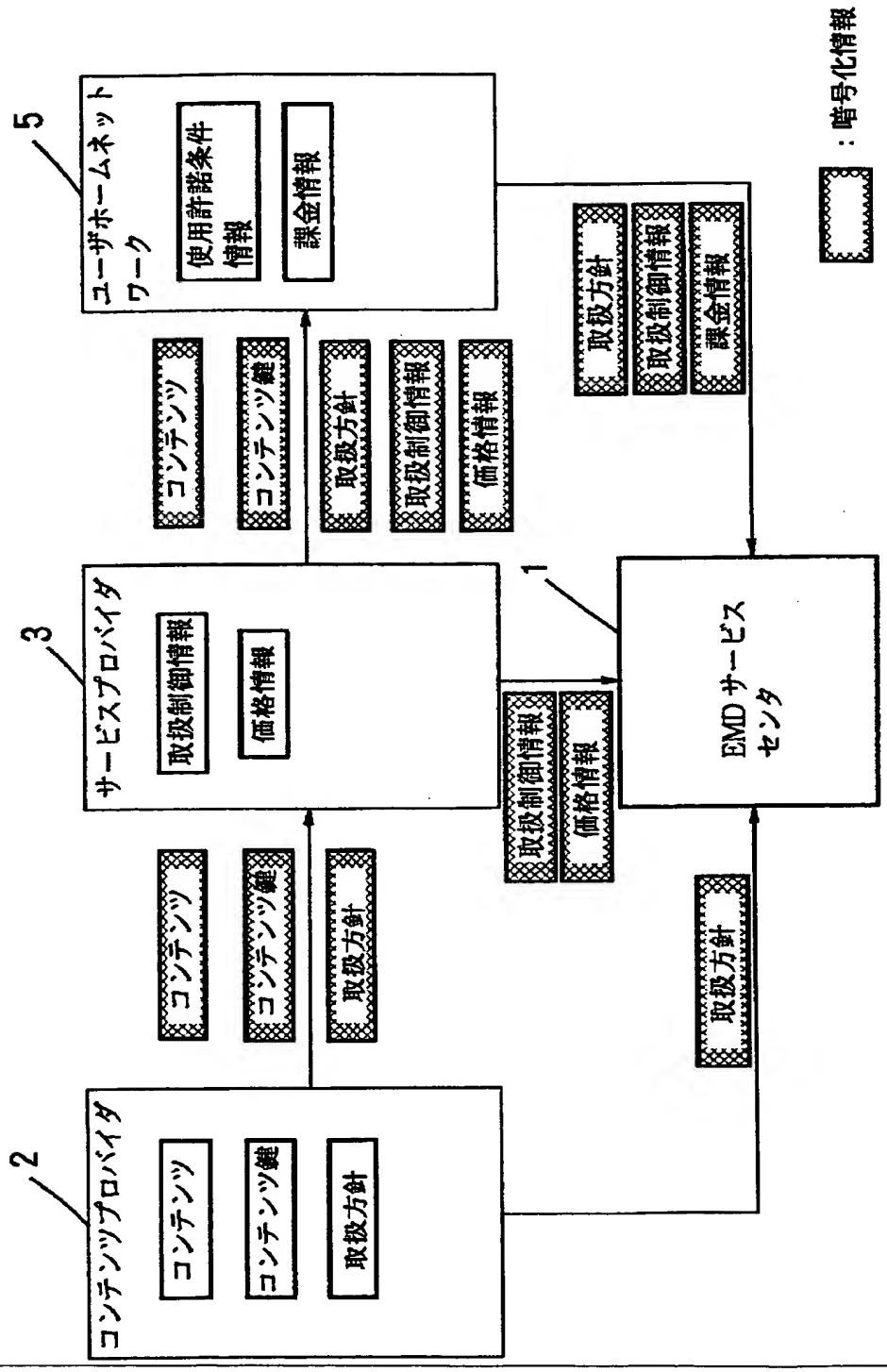
【図２２】


コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵Kco
コンテンツ
配送用鍵Kd
コンテンツ鍵Kco
取扱方針
取扱制御情報
価格情報
サービスプロバイダの秘密鍵Kssp
署名
ハッシュ関数
コンテンツ鍵Kco
コンテンツ
配送用鍵Kd
コンテンツ鍵Kco
取扱方針
取扱制御情報
価格情報

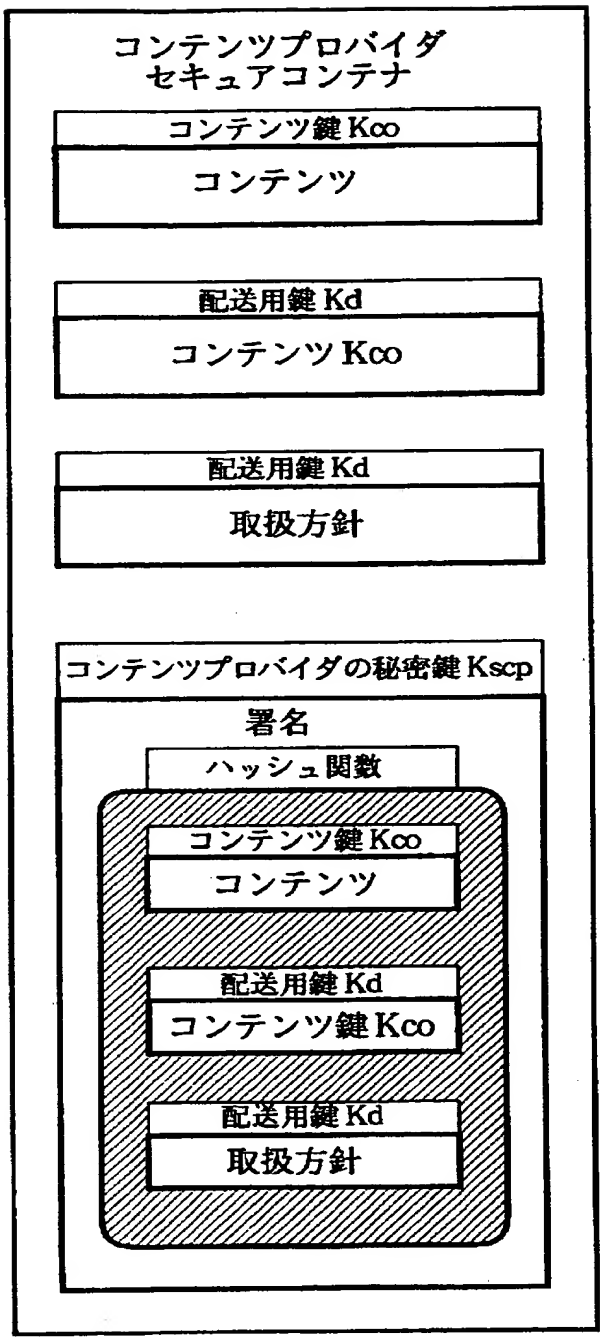
【図２３】


再生：YES；
シングルコピー：NO；
マルチコピー：YES
(A) 取扱方針
(B) 取扱制御情報および価格情報
利用内容 | 再生 | シングルコピー | マルチコピー
可／否 | 1 | 0 | 1
価格 | 150円 | − | 80円
(C) 使用許諾条件情報
利用内容 | 再生 | シングルコピー | マルチコピー
可／否 | 1 | 0 | 0

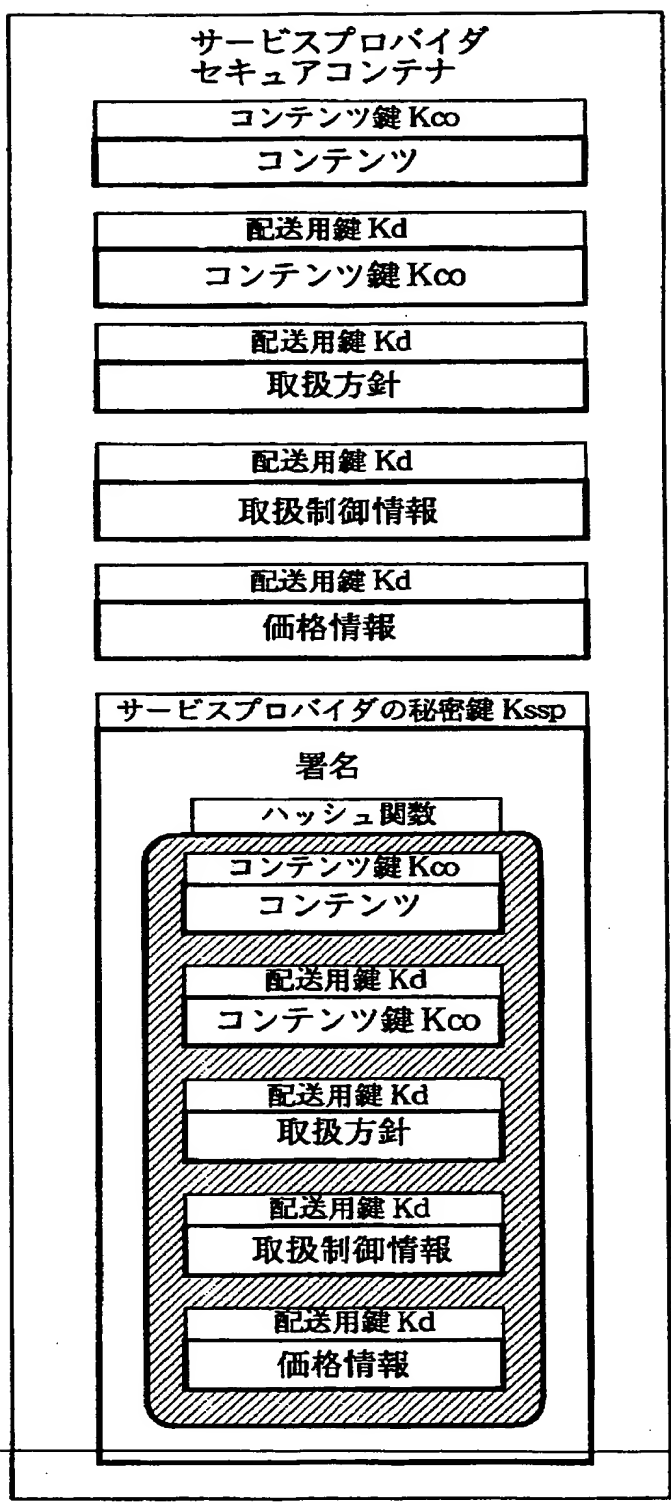
【図２４】


：暗号化情報
5
ユーザホームネットワーク
使用許諾条件情報
課金情報
コンテンツ
コンテンツ鍵
取扱方針
取扱制御情報
価格情報
取扱方針
取扱制御情報
課金情報
3
サービスプロバイダ
取扱制御情報
価格情報
1
EMDサービスセンタ
取扱制御情報
価格情報
コンテンツ
コンテンツ鍵
取扱方針
取扱方針
2
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
取扱方針

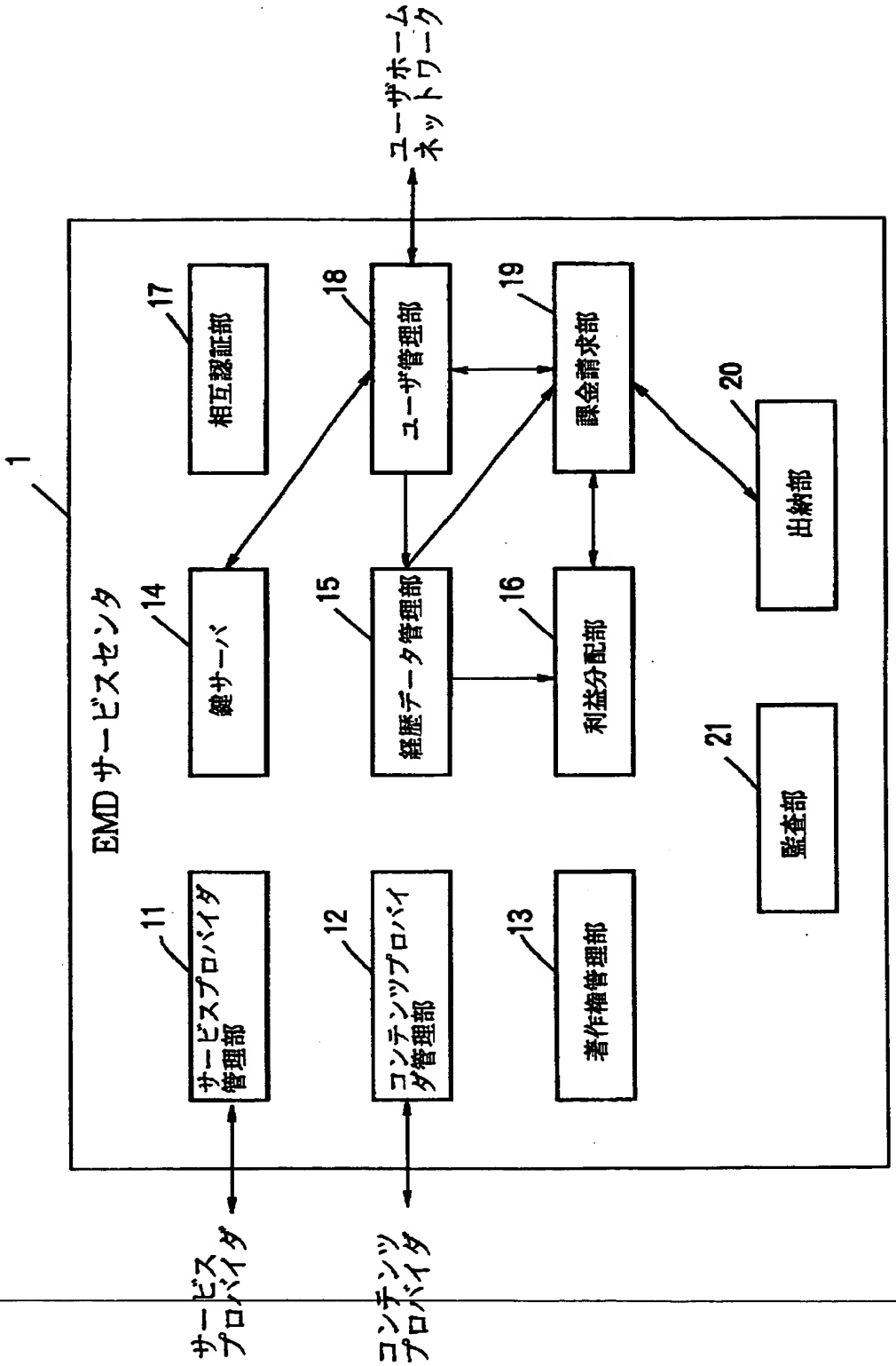
【図２５】


コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ Kco
配送用鍵 Kd
取扱方針
コンテンツプロバイダの秘密鍵 Kscp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
配送用鍵 Kd
取扱方針

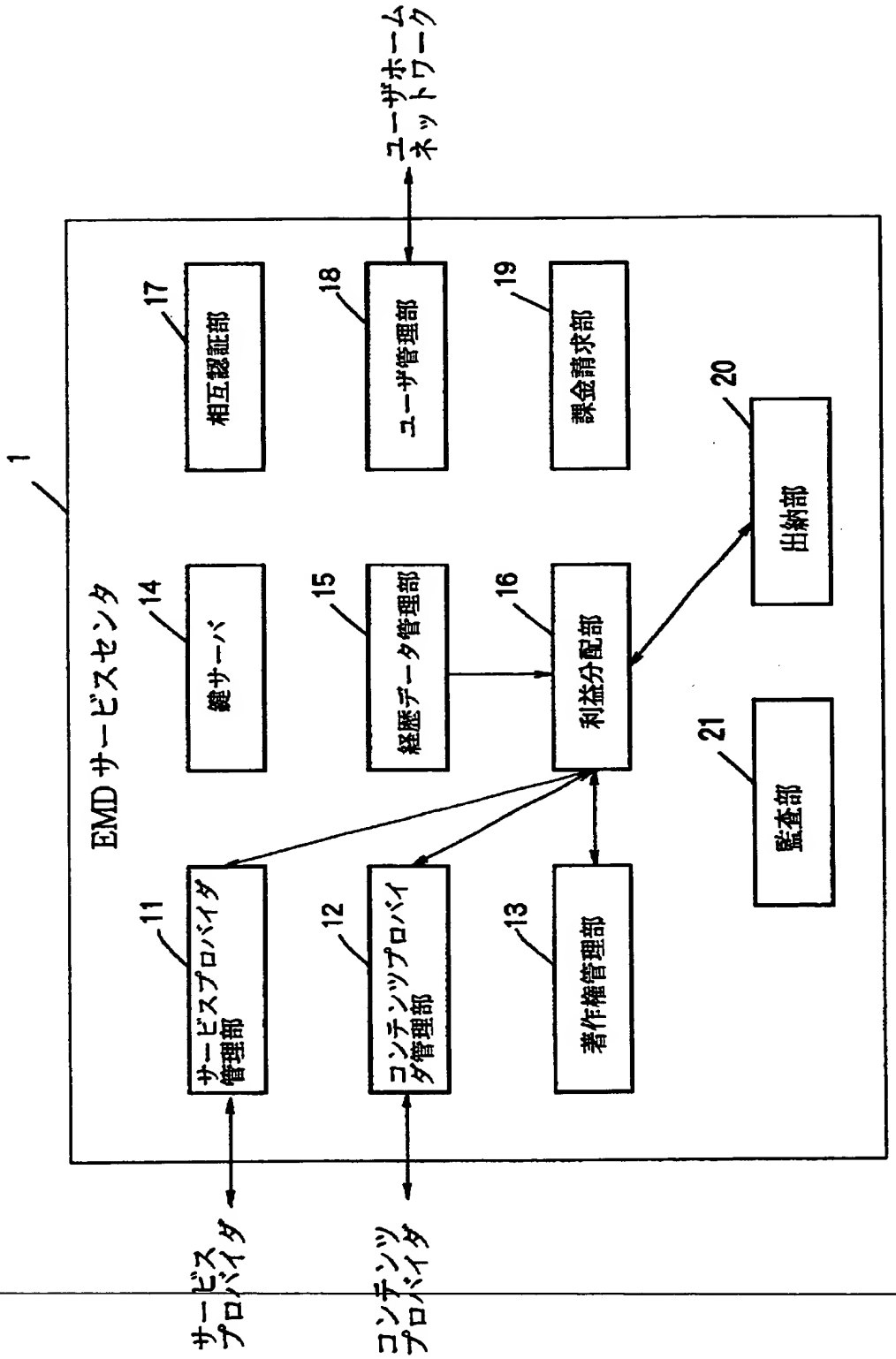
【図２６】


サービスプロバイダ
セキュアコンテナ
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
配送用鍵 Kd
取扱方針
配送用鍵 Kd
取扱制御情報
配送用鍵 Kd
価格情報
サービスプロバイダの秘密鍵 Kssp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
配送用鍵 Kd
取扱方針
配送用鍵 Kd
取扱制御情報
配送用鍵 Kd
価格情報

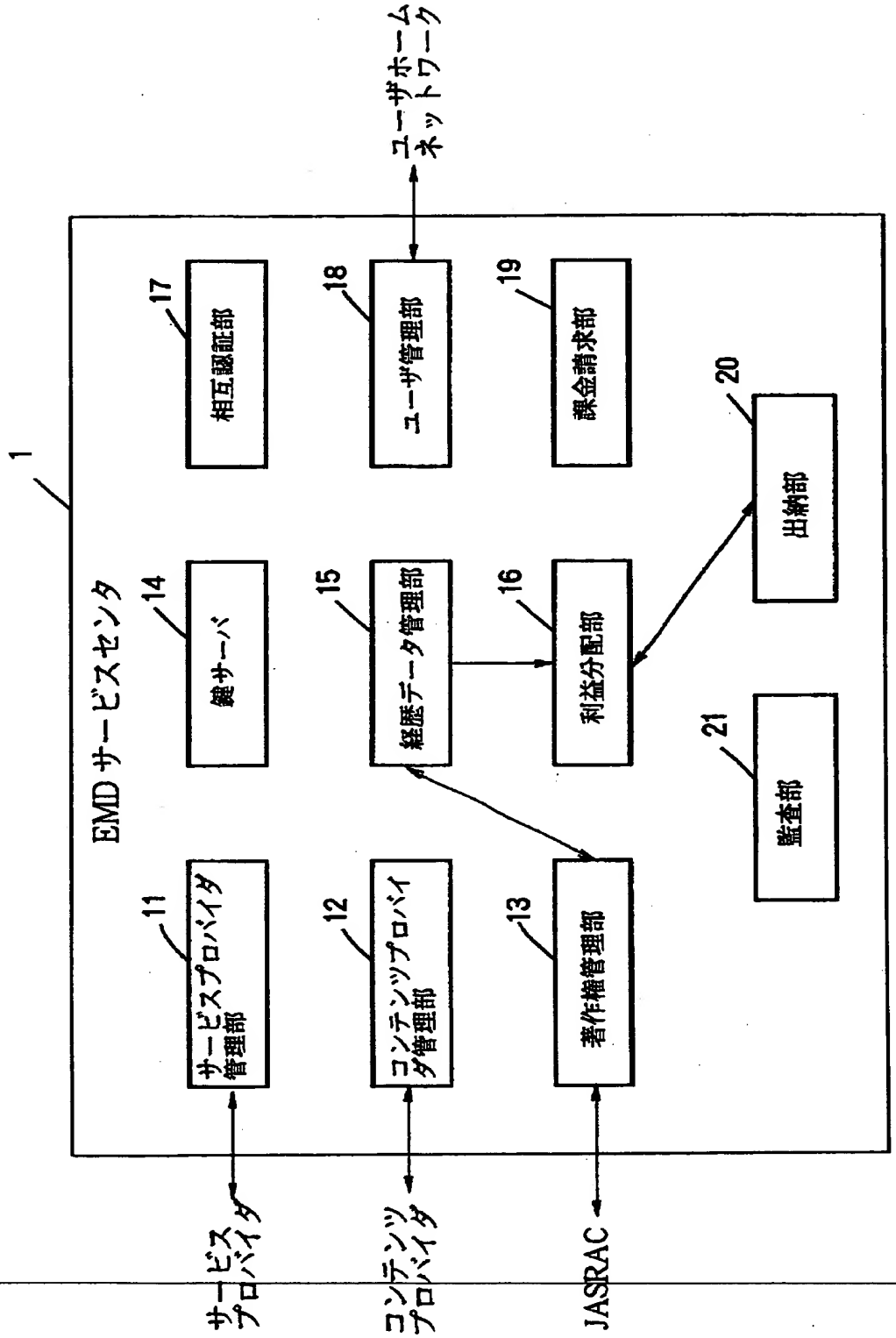
【図２７】


ユーザホームネットワーク
1
EMDサービスセンタ
相互認証部
17
ユーザ管理部
18
課金請求部
19
出納部
20
鍵サーバ
14
経歴データ管理部
15
利益分配部
16
監査部
21
サービスプロバイダ管理部
11
コンテンツプロバイダ管理部
12
著作権管理部
13
サービスプロバイダ
コンテンツプロバイダ

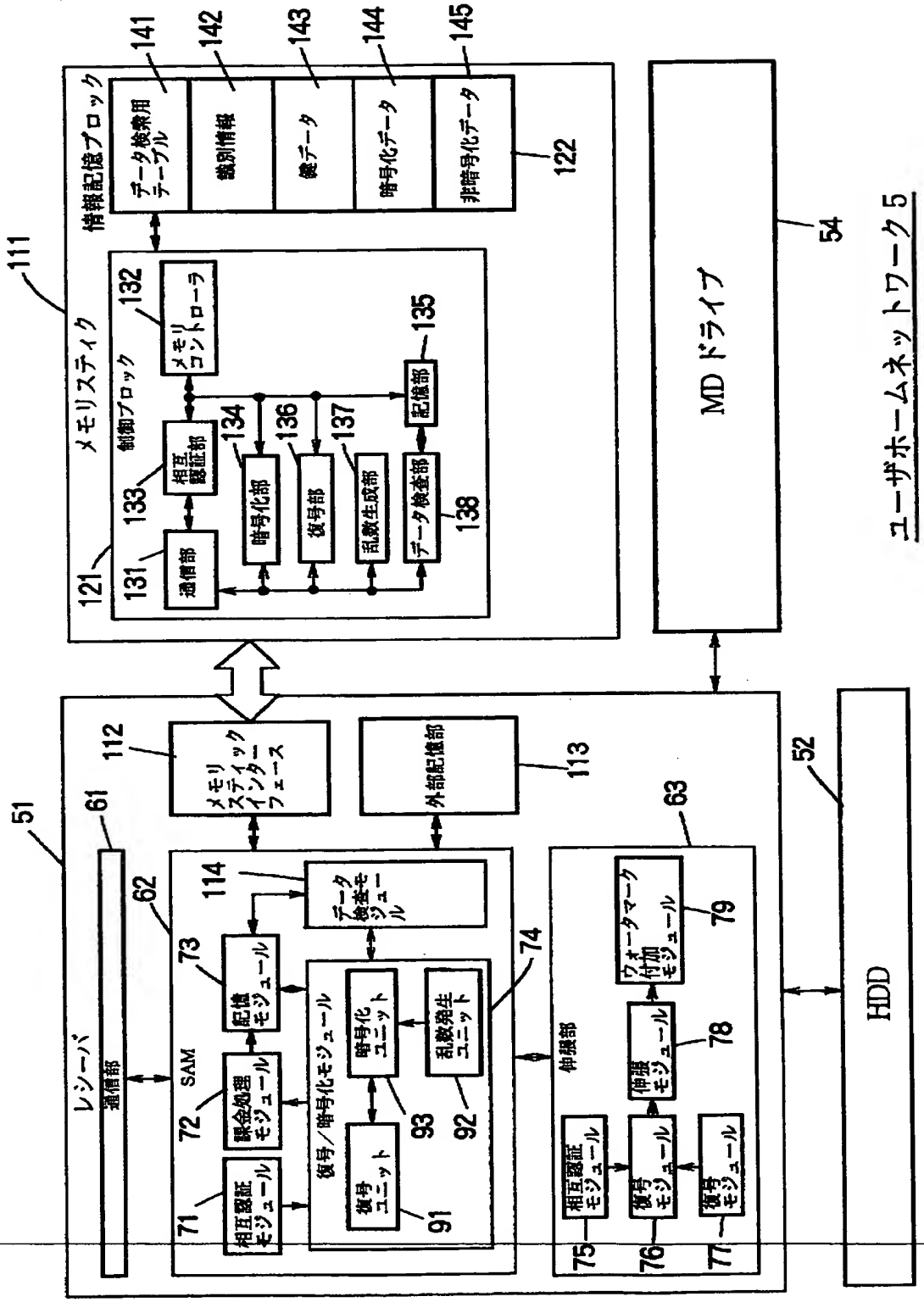
【図２８】


ユーザホームネットワーク
EMDサービスセンタ
1
相互認証部
17
ユーザ管理部
18
課金請求部
19
出納部
20
鍵サーバ
14
経歴データ管理部
15
利益分配部
16
監査部
21
サービスプロバイダ管理部
11
コンテンツプロバイダ管理部
12
著作権管理部
13
サービスプロバイダ
コンテンツプロバイダ

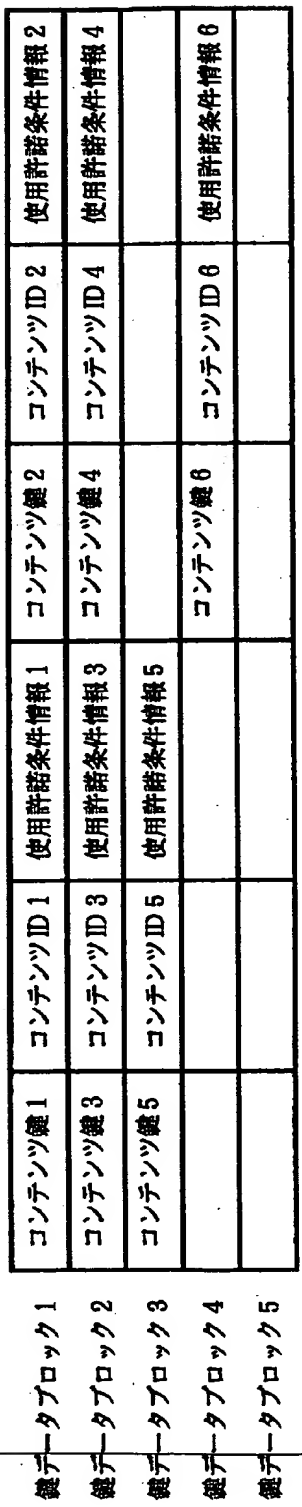
【図２９】


ユーザホーム
ネットワーク
1
EMD サービスセンタ
17
相互認証部
18
ユーザ管理部
19
課金請求部
20
出納部
14
鍵サーバ
15
経歴データ管理部
16
利益分配部
21
監査部
11
サービスプロバイダ
管理部
12
コンテンツプロバイ
ダ管理部
13
著作権管理部
サービス
プロバイダ
コンテンツ
プロバイダ
JASRAC

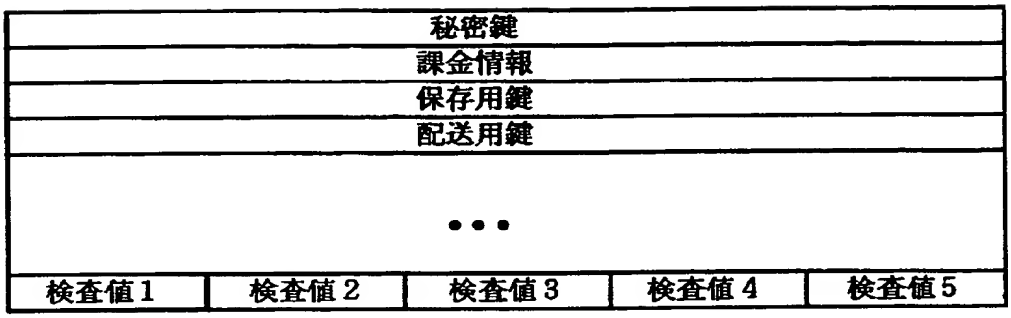
【図３０】


ユーザホームネットワーク5
メモリスティック
111
情報記憶ブロック
141
データ検索用テーブル
142
識別情報
143
鍵データ
144
暗号化データ
145
非暗号化データ
122
制御ブロック
132
メモリコントローラ
133
相互認証部
134
暗号化部
136
復号部
137
乱数生成部
135
記憶部
138
データ検査部
131
通信部
121
MDドライブ
54
HDD
52
51
メモリスティックインターフェース
112
外部記憶部
113
63
61
62
114
データ検査モジュール
73
記憶モジュール
SAM
72
課金処理モジュール
71
相互認証モジュール
復号／暗号化モジュール
暗号化ユニット
乱数発生ユニット
復号ユニット
93
92
91
74
レシーバ
通信部
伸張部
ウォータマーク付加モジュール
79
伸張モジュール
78
相互認証モジュール
75
復号モジュール
76
復号モジュール
77

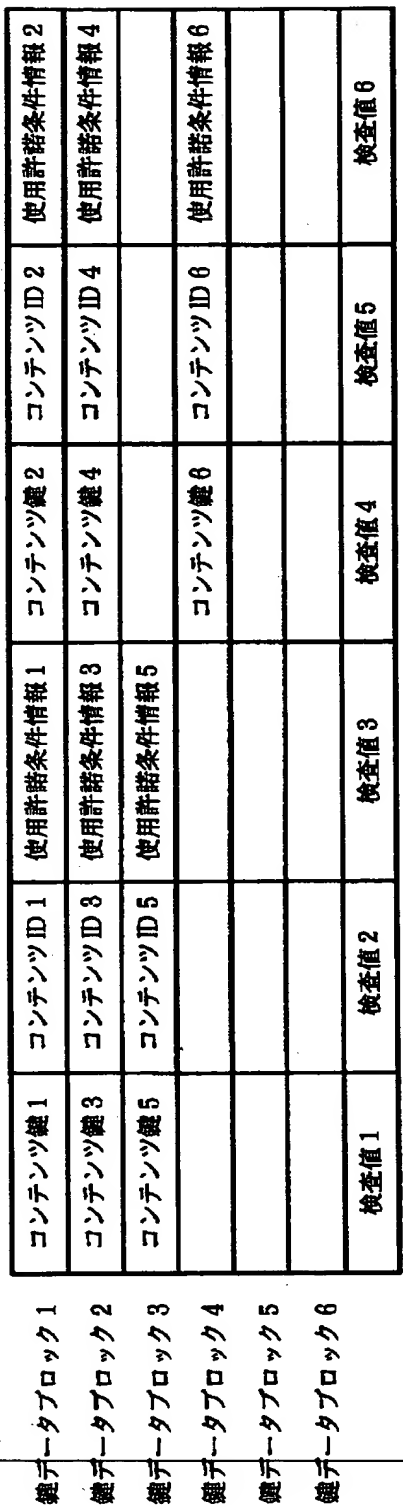
【図３１】


鍵データブロック１
鍵データブロック２
鍵データブロック３
鍵データブロック４
鍵データブロック５
コンテンツ鍵１
コンテンツＩＤ１
使用許諾条件情報１
コンテンツ鍵２
コンテンツＩＤ２
使用許諾条件情報２
コンテンツ鍵３
コンテンツＩＤ３
使用許諾条件情報３
コンテンツ鍵４
コンテンツＩＤ４
使用許諾条件情報４
コンテンツ鍵５
コンテンツＩＤ５
使用許諾条件情報５
コンテンツ鍵６
コンテンツＩＤ６
使用許諾条件情報６

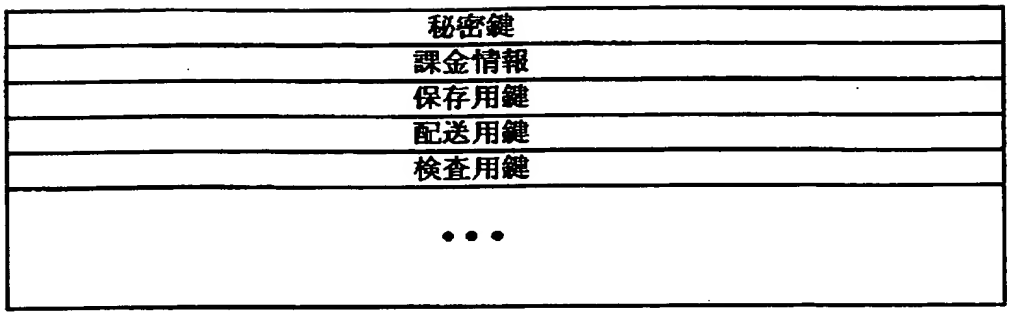
【図３２】



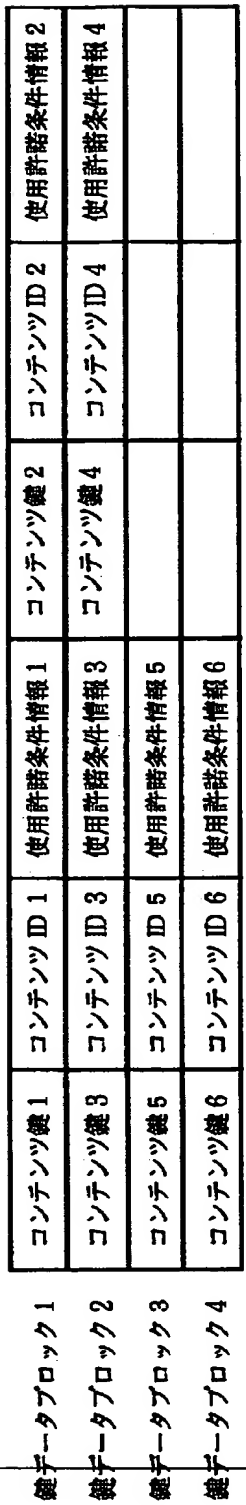
【図３３】


鍵データブロック１
鍵データブロック２
鍵データブロック３
鍵データブロック４
鍵データブロック５
鍵データブロック６
コンテンツ鍵１
コンテンツＩＤ１
使用許諾条件情報１
コンテンツ鍵２
コンテンツＩＤ２
使用許諾条件情報２
コンテンツ鍵３
コンテンツＩＤ３
使用許諾条件情報３
コンテンツ鍵４
コンテンツＩＤ４
使用許諾条件情報４
コンテンツ鍵５
コンテンツＩＤ５
使用許諾条件情報５
コンテンツ鍵６
コンテンツＩＤ６
使用許諾条件情報６
検査値１
検査値２
検査値３
検査値４
検査値５
検査値６

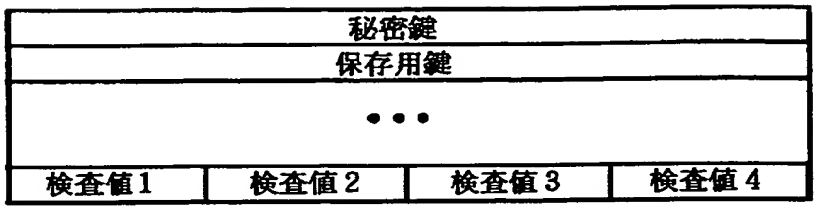
【図３４】



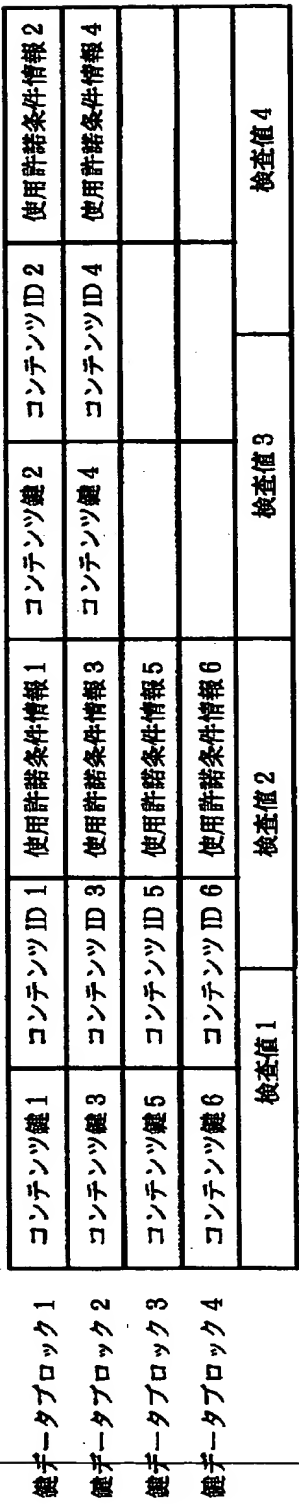
【図３５】


鍵データブロック１
鍵データブロック２
鍵データブロック３
鍵データブロック４
コンテンツ鍵１
コンテンツＩＤ１
使用許諾条件情報１
コンテンツ鍵２
コンテンツＩＤ２
使用許諾条件情報２
コンテンツ鍵３
コンテンツＩＤ３
使用許諾条件情報３
コンテンツ鍵４
コンテンツＩＤ４
使用許諾条件情報４
コンテンツ鍵５
コンテンツＩＤ５
使用許諾条件情報５
コンテンツ鍵６
コンテンツＩＤ６
使用許諾条件情報６

【図３６】



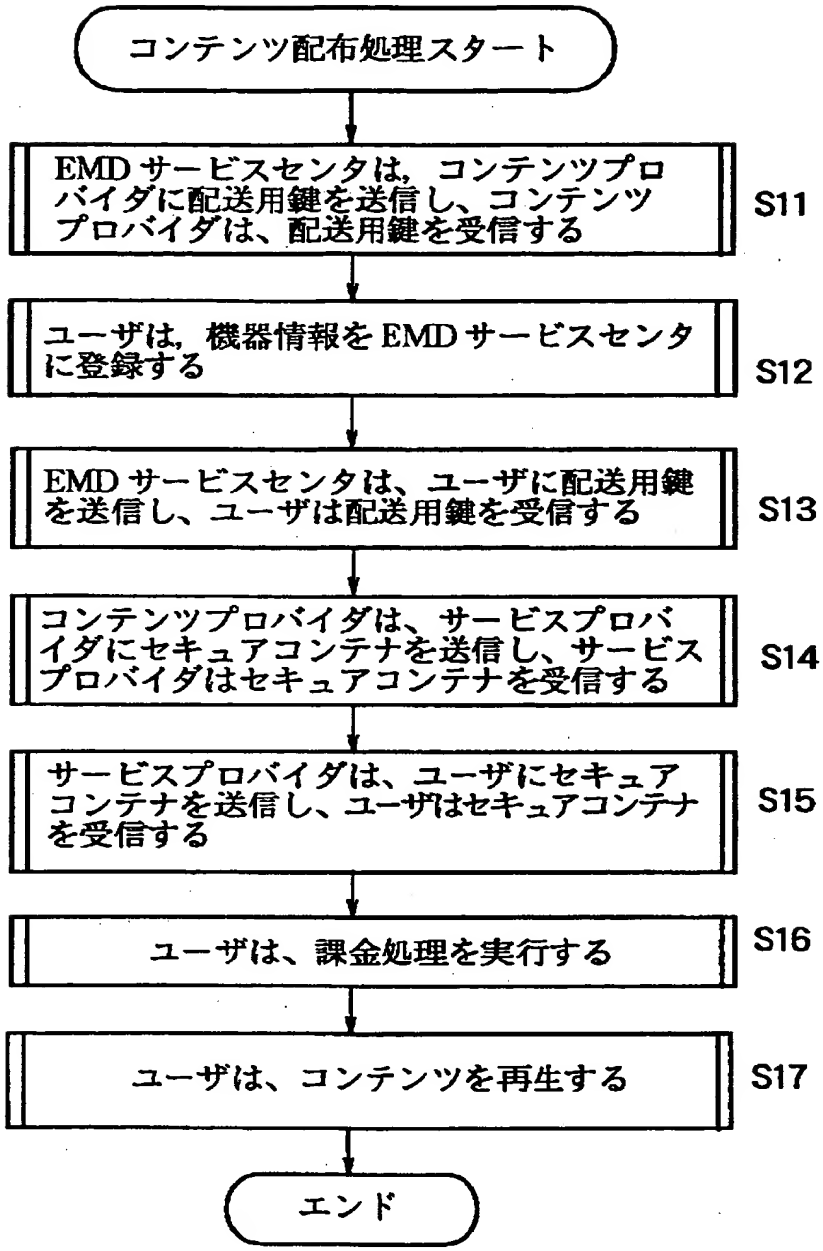
【図３７】


鍵データブロック１
鍵データブロック２
鍵データブロック３
鍵データブロック４
コンテンツ鍵１
コンテンツＩＤ１
使用許諾条件情報１
コンテンツ鍵２
コンテンツＩＤ２
使用許諾条件情報２
コンテンツ鍵３
コンテンツＩＤ３
使用許諾条件情報３
コンテンツ鍵４
コンテンツＩＤ４
使用許諾条件情報４
コンテンツ鍵５
コンテンツＩＤ５
使用許諾条件情報５
コンテンツ鍵６
コンテンツＩＤ６
使用許諾条件情報６
検査値１
検査値２
検査値３
検査値４

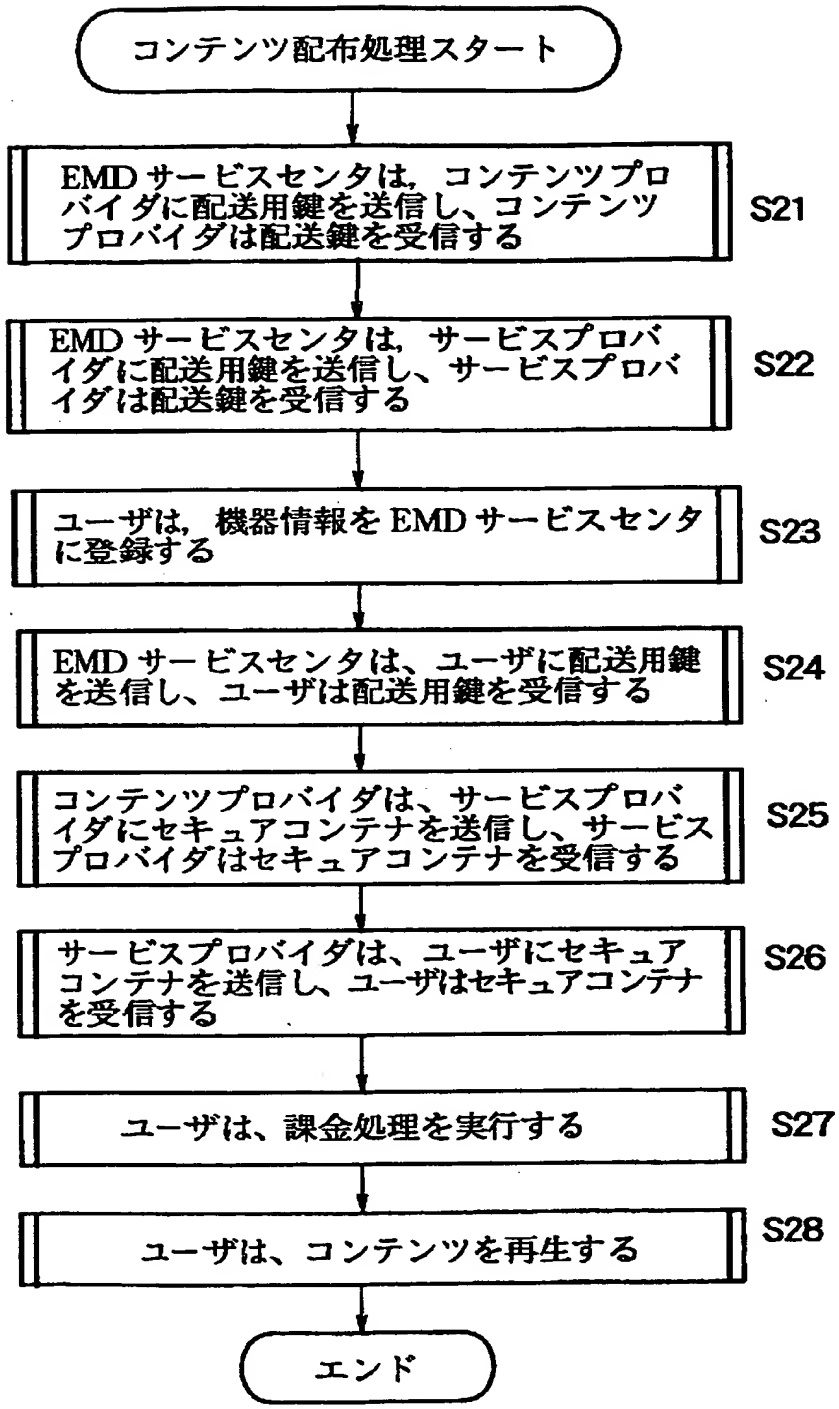
【図３８】

秘密鍵
検査用鍵
保存用鍵
・・・

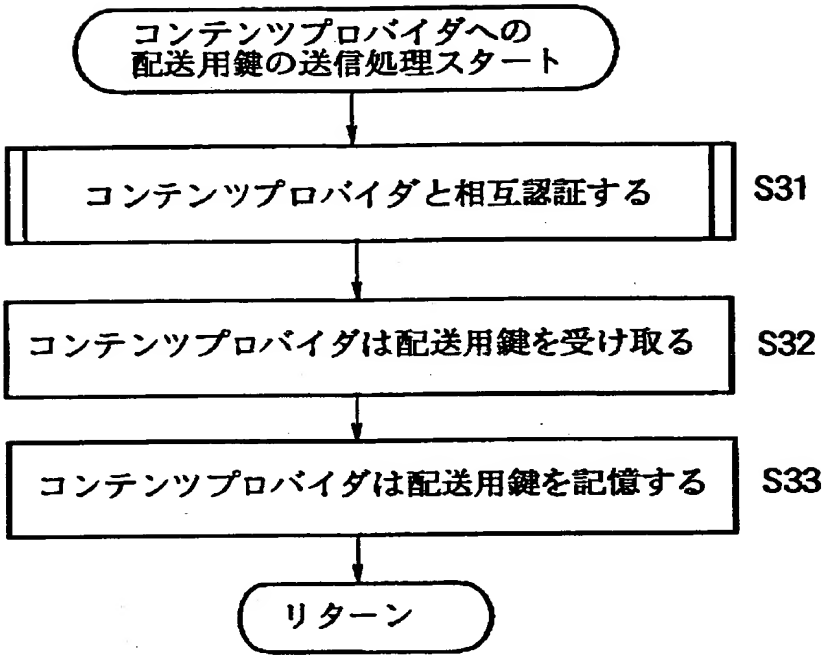
【図３９】


コンテンツ配布処理スタート
EMDサービスセンタは，コンテンツプロバイダに配送用鍵を送信し、コンテンツプロバイダは、配送用鍵を受信する
S11
ユーザは，機器情報をEMDサービスセンタに登録する
S12
EMDサービスセンタは、ユーザに配送用鍵を送信し、ユーザは配送用鍵を受信する
S13
コンテンツプロバイダは、サービスプロバイダにセキュアコンテナを送信し、サービスプロバイダはセキュアコンテナを受信する
S14
サービスプロバイダは、ユーザにセキュアコンテナを送信し、ユーザはセキュアコンテナを受信する
S15
ユーザは、課金処理を実行する
S16
ユーザは、コンテンツを再生する
S17
エンド

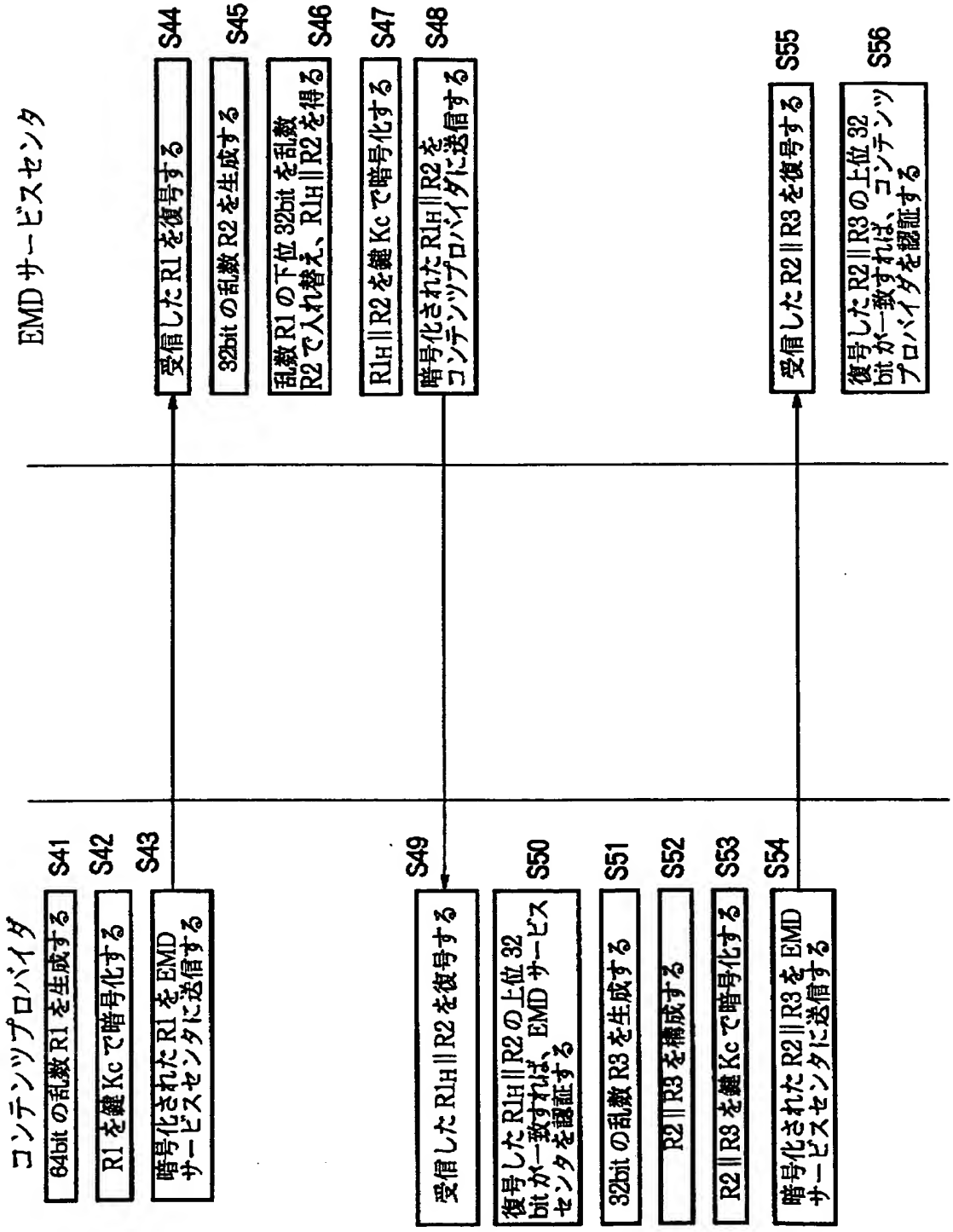
【図４０】


コンテンツ配布処理スタート
EMDサービスセンタは，コンテンツプロバイダに配送用鍵を送信し、コンテンツプロバイダは配送鍵を受信する
S21
EMDサービスセンタは，サービスプロバイダに配送用鍵を送信し、サービスプロバイダは配送鍵を受信する
S22
ユーザは，機器情報をEMDサービスセンタに登録する
S23
EMDサービスセンタは、ユーザに配送用鍵を送信し、ユーザは配送用鍵を受信する
S24
コンテンツプロバイダは、サービスプロバイダにセキュアコンテナを送信し、サービスプロバイダはセキュアコンテナを受信する
S25
サービスプロバイダは、ユーザにセキュアコンテナを送信し、ユーザはセキュアコンテナを受信する
S26
ユーザは、課金処理を実行する
S27
ユーザは、コンテンツを再生する
S28
エンド

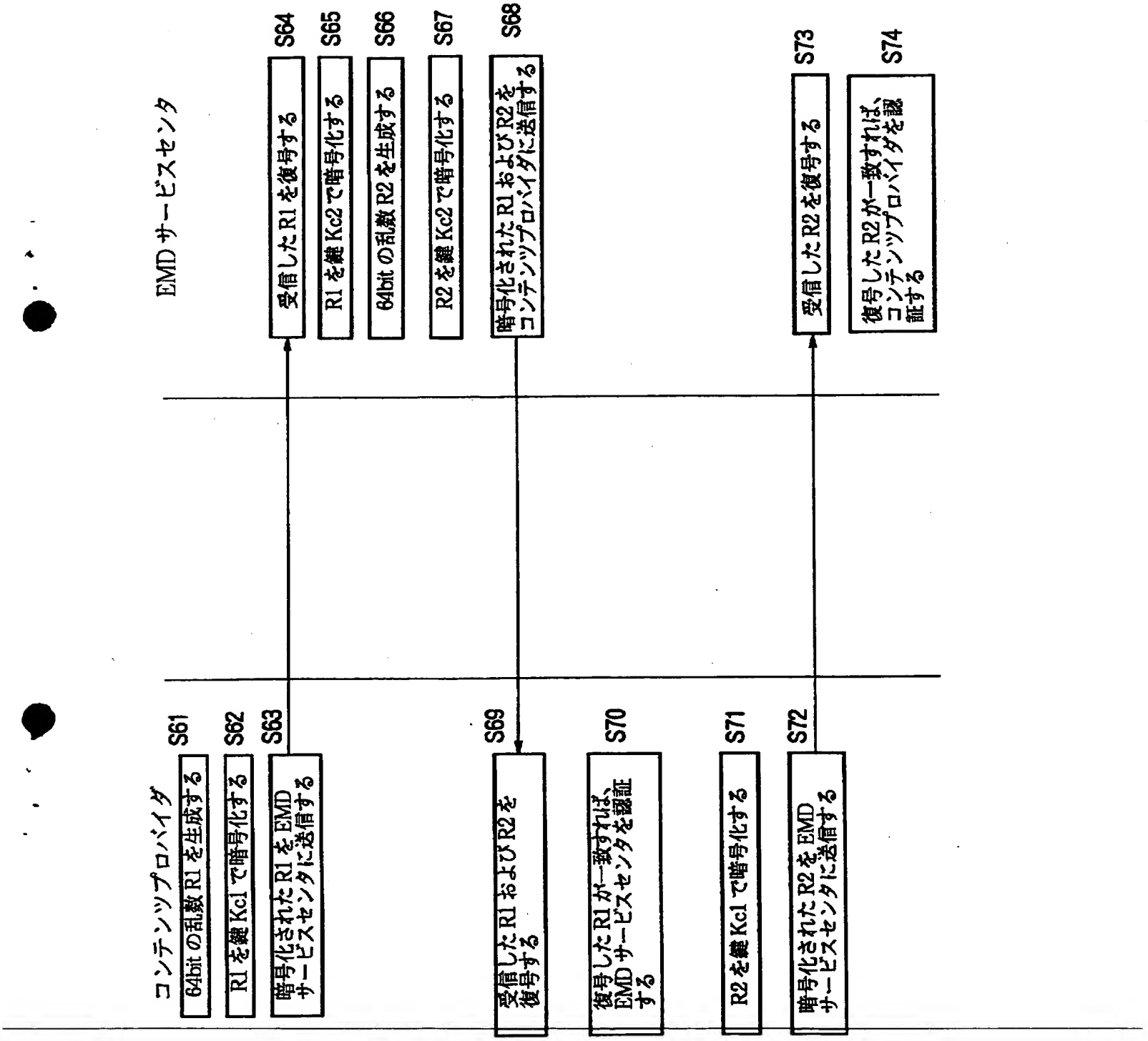
【図４１】


コンテンツプロバイダへの
配送用鍵の送信処理スタート
コンテンツプロバイダと相互認証する
S31
コンテンツプロバイダは配送用鍵を受け取る
S32
コンテンツプロバイダは配送用鍵を記憶する
S33
リターン

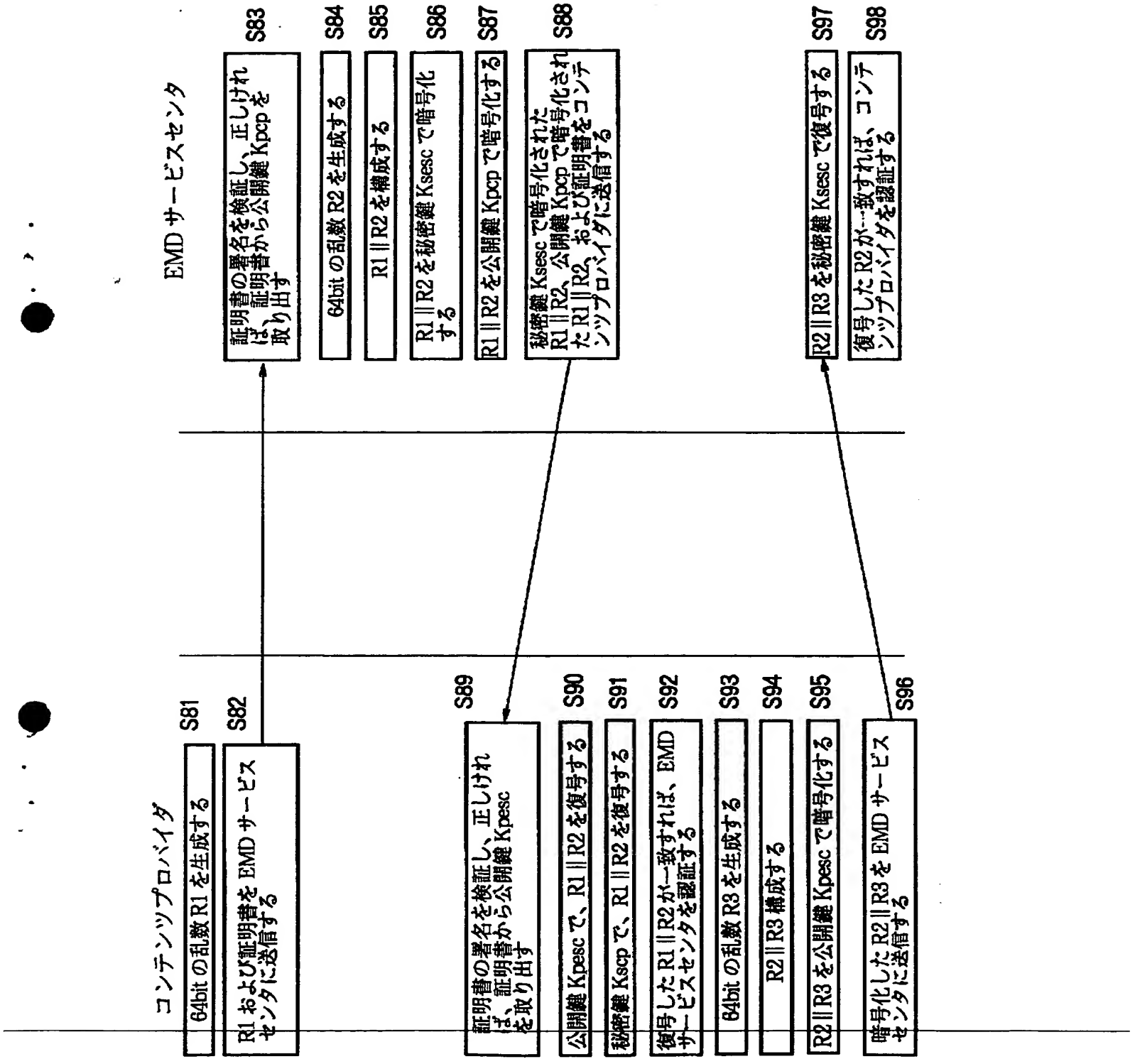
【図４２】


EMDサービスセンタ
コンテンツプロバイダ
S41
84bitの乱数R1を生成する
S42
R1を鍵Kcで暗号化する
S43
暗号化されたR1をEMDサービスセンタに送信する
S44
受信したR1を復号する
S45
32bitの乱数R2を生成する
S46
乱数R1の下位32bitを乱数R2で入れ替え、R1H||R2を得る
S47
R1H||R2を鍵Kcで暗号化する
S48
暗号化されたR1H||R2をコンテンツプロバイダに送信する
S49
受信したR1H||R2を復号する
S50
復号したR1H||R2の上位32bitが一致すれば、EMDサービスセンタを認証する
S51
32bitの乱数R3を生成する
S52
R2||R3を構成する
S53
R2||R3を鍵Kcで暗号化する
S54
暗号化されたR2||R3をEMDサービスセンタに送信する
S55
受信したR2||R3を復号する
S56
復号したR2||R3の上位32bitが一致すれば、コンテンツプロバイダを認証する

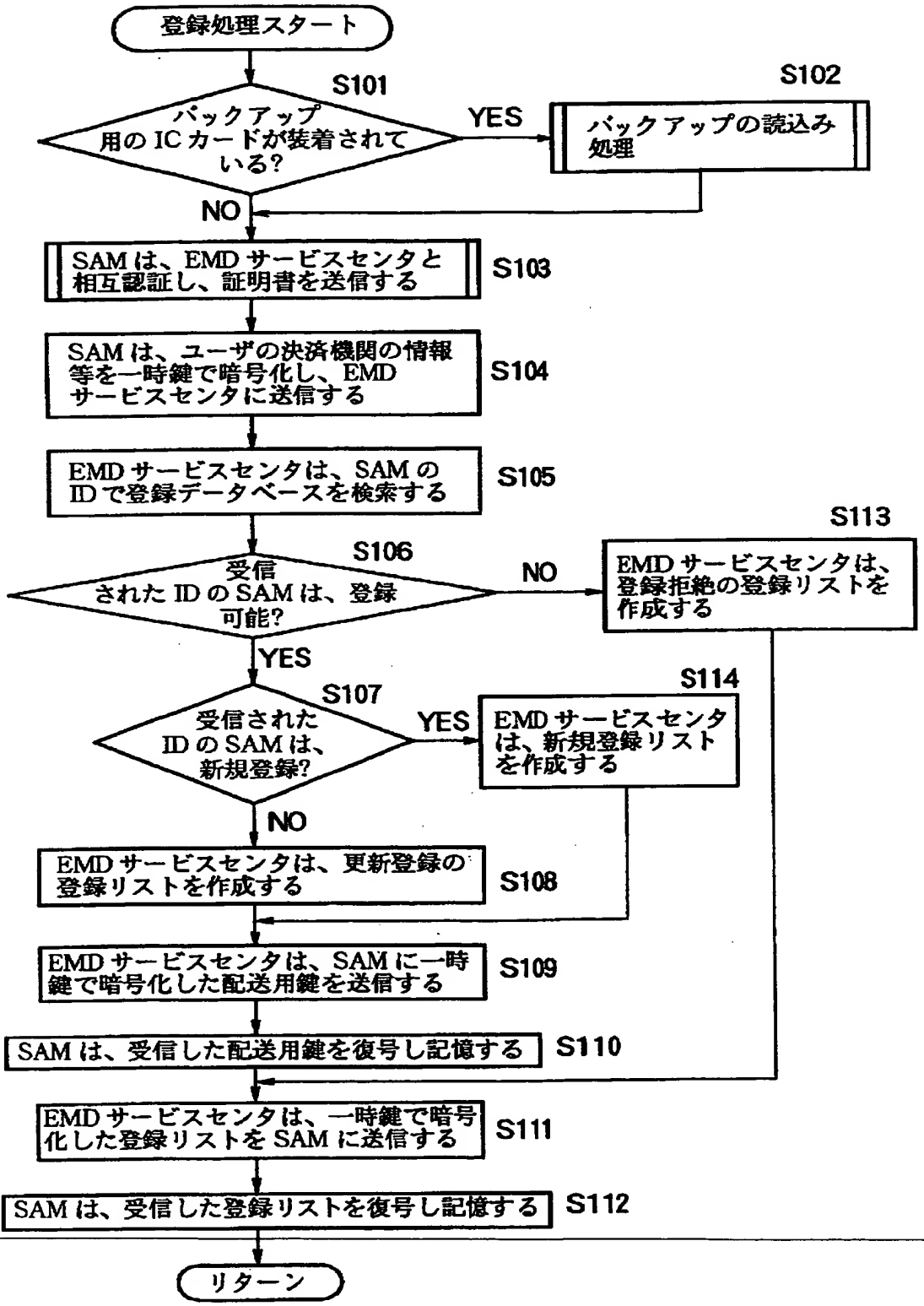
【図４３】


EMDサービスセンタ
コンテンツプロバイダ
S61
64bitの乱数R1を生成する
S62
R1を鍵Kc1で暗号化する
S63
暗号化されたR1をEMDサービスセンタに送信する
S64
受信したR1を復号する
S65
R1を鍵Kc2で暗号化する
S66
64bitの乱数R2を生成する
S67
R2を鍵Kc2で暗号化する
S68
暗号化されたR1およびR2をコンテンツプロバイダに送信する
S69
受信したR1およびR2を復号する
S70
復号したR1が一致すれば、EMDサービスセンタを認証する
S71
R2を鍵Kc1で暗号化する
S72
暗号化されたR2をEMDサービスセンタに送信する
S73
受信したR2を復号する
S74
復号したR2が一致すれば、コンテンツプロバイダを認証する

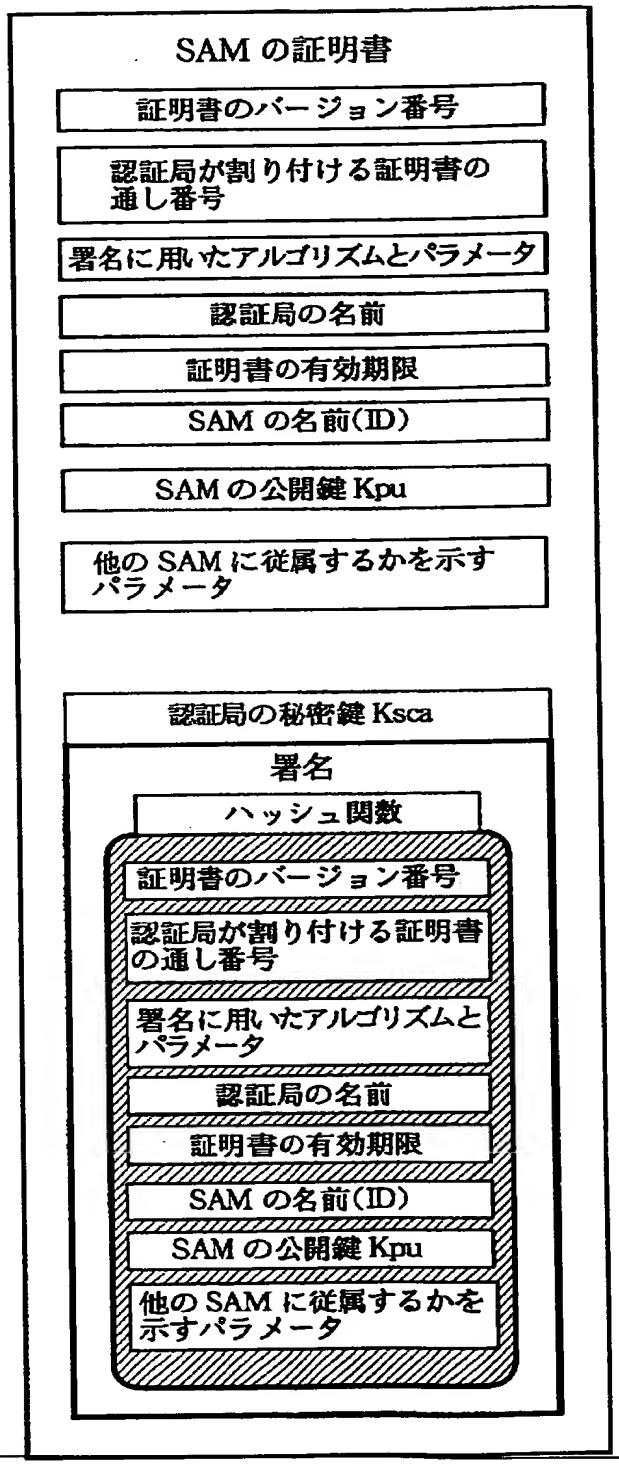
【図４４】


EMD サービスセンタ
コンテンツプロバイダ
S81
64bit の乱数 R1 を生成する
S82
R1 および証明書を EMD サービスセンタに送信する
S83
証明書の署名を検証し、正しければ、証明書から公開鍵 Kpcp を取り出す
S84
64bit の乱数 R2 を生成する
S85
R1 || R2 を構成する
S86
R1 || R2 を秘密鍵 Ksesc で暗号化する
S87
R1 || R2 を公開鍵 Kpcp で暗号化する
S88
秘密鍵 Ksesc で暗号化された R1 || R2、公開鍵 Kpcp で暗号化された R1 || R2、および証明書をコンテンツプロバイダに送信する
S89
証明書の署名を検証し、正しければ、証明書から公開鍵 Kpesc を取り出す
S90
公開鍵 Kpesc で、R1 || R2 を復号する
S91
秘密鍵 Kscp で、R1 || R2 を復号する
S92
復号した R1 || R2 が一致すれば、EMD サービスセンタを認証する
S93
64bit の乱数 R3 を生成する
S94
R2 || R3 構成する
S95
R2 || R3 を公開鍵 Kpesc で暗号化する
S96
暗号化した R2 || R3 を EMD サービスセンタに送信する
S97
R2 || R3 を秘密鍵 Ksesc で復号する
S98
復号した R2 が一致すれば、コンテンツプロバイダを認証する

【図４５】


登録処理スタート
S101
バックアップ用のICカードが装着されている?
YES
S102
バックアップの読込み処理
NO
SAMは、EMDサービスセンタと相互認証し、証明書を送信する
S103
SAMは、ユーザの決済機関の情報等を一時鍵で暗号化し、EMDサービスセンタに送信する
S104
EMDサービスセンタは、SAMのIDで登録データベースを検索する
S105
S106
受信されたIDのSAMは、登録可能?
NO
S113
EMDサービスセンタは、登録拒絶の登録リストを作成する
YES
S107
受信されたIDのSAMは、新規登録?
YES
S114
EMDサービスセンタは、新規登録リストを作成する
NO
EMDサービスセンタは、更新登録の登録リストを作成する
S108
EMDサービスセンタは、SAMに一時鍵で暗号化した配送用鍵を送信する
S109
SAMは、受信した配送用鍵を復号し記憶する
S110
EMDサービスセンタは、一時鍵で暗号化した登録リストをSAMに送信する
S111
SAMは、受信した登録リストを復号し記憶する
S112
リターン

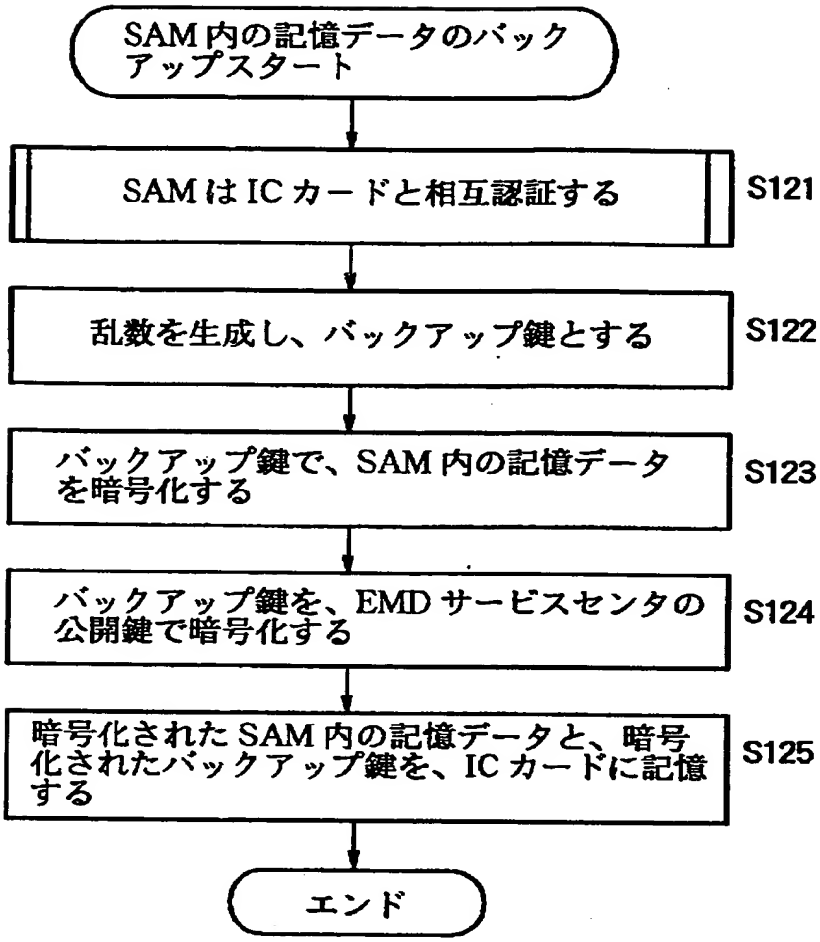
【図４６】


SAM の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
SAM の名前(ID)
SAM の公開鍵 Kpu
他の SAM に従属するかを示すパラメータ
認証局の秘密鍵 Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
SAM の名前(ID)
SAM の公開鍵 Kpu
他の SAM に従属するかを示すパラメータ

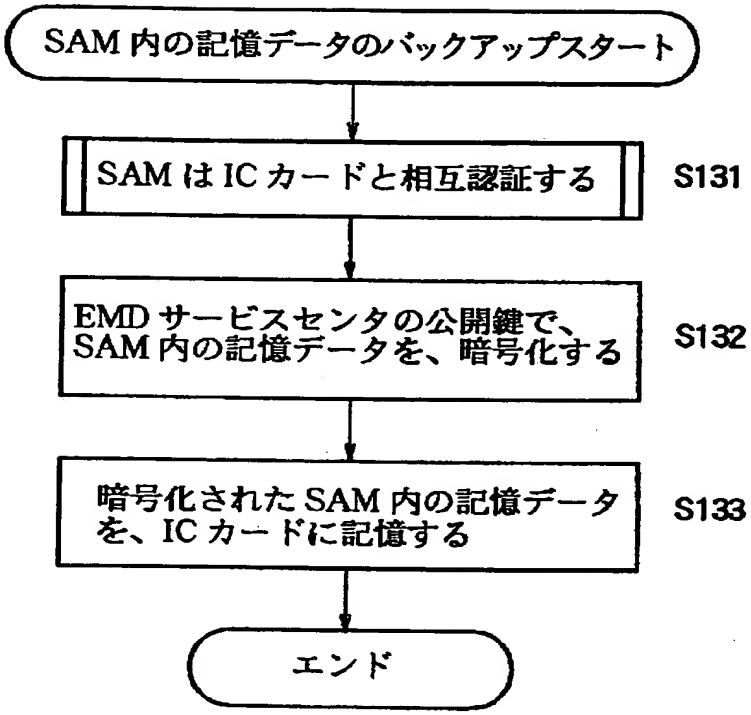
【図４７】

SAMのID (64bit)	登録拒絶フラグ (1bit)	ステータスフラグ (4bit)	コンディションフラグ (1bit)	署名
0000000000000001h	1	0000	0	xxxxxxxxxx
0000000000000002h	1	1010	1	xxxxxxxxxx
0000000000000003h	1	1100	1	xxxxxxxxxx
000000000000000Ah	0	0000	1	xxxxxxxxxx

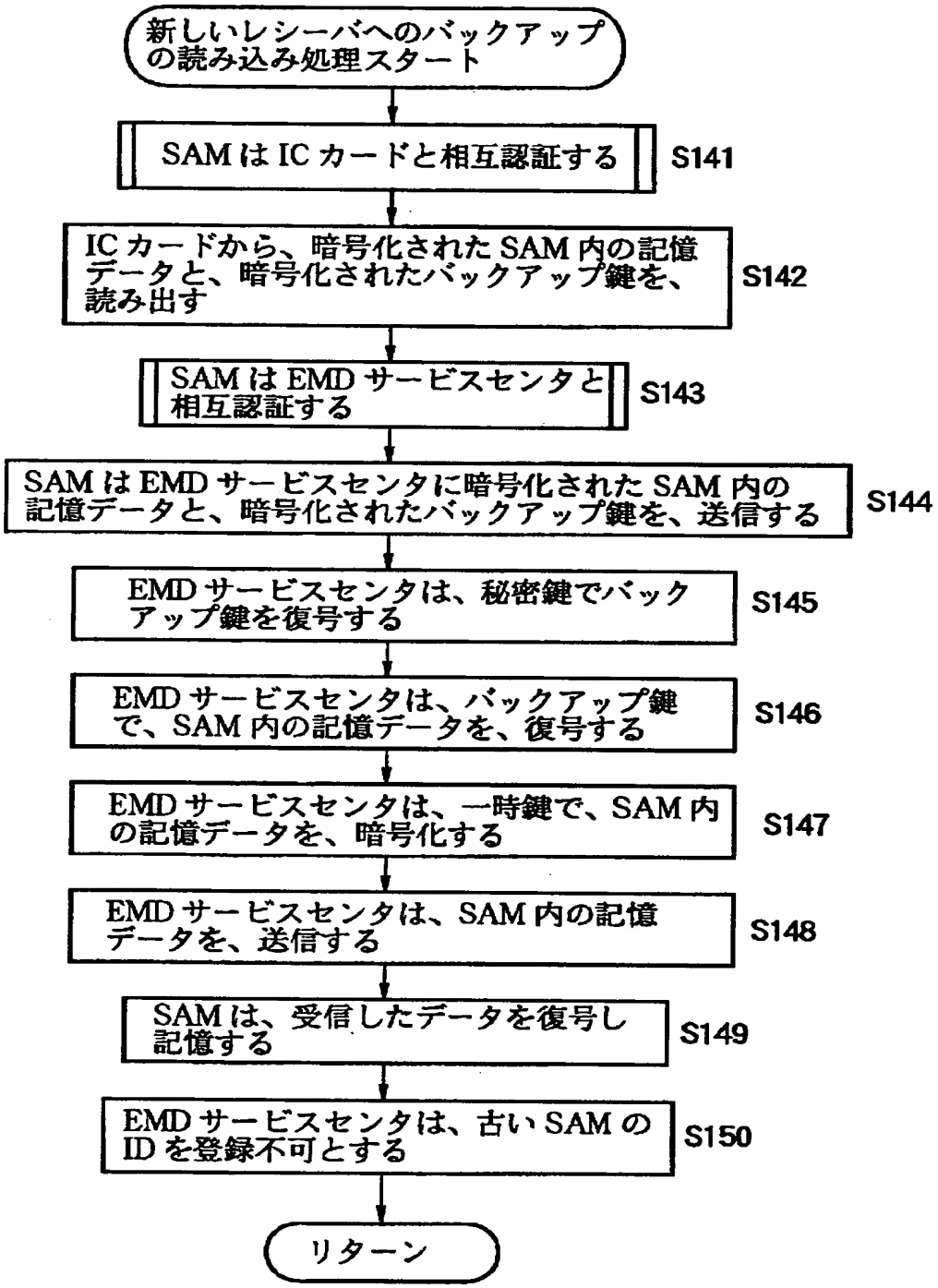
【図４８】


SAM内の記憶データのバックアップスタート
SAMはICカードと相互認証する
S121
乱数を生成し、バックアップ鍵とする
S122
バックアップ鍵で、SAM内の記憶データを暗号化する
S123
バックアップ鍵を、EMDサービスセンタの公開鍵で暗号化する
S124
暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、ICカードに記憶する
S125
エンド

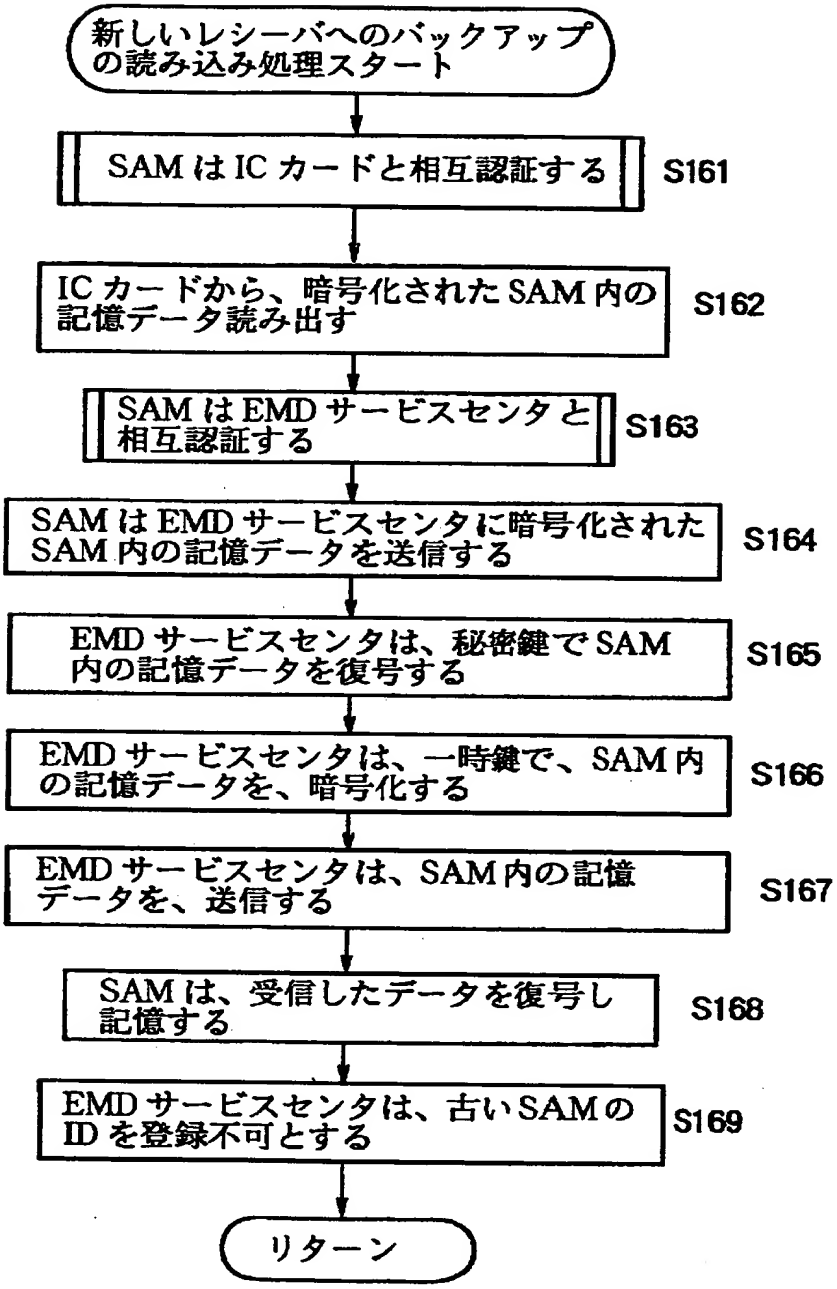
【図４９】


SAM 内の記憶データのバックアップスタート
SAM は IC カードと相互認証する
S131
EMD サービスセンタの公開鍵で、SAM 内の記憶データを、暗号化する
S132
暗号化された SAM 内の記憶データを、IC カードに記憶する
S133
エンド

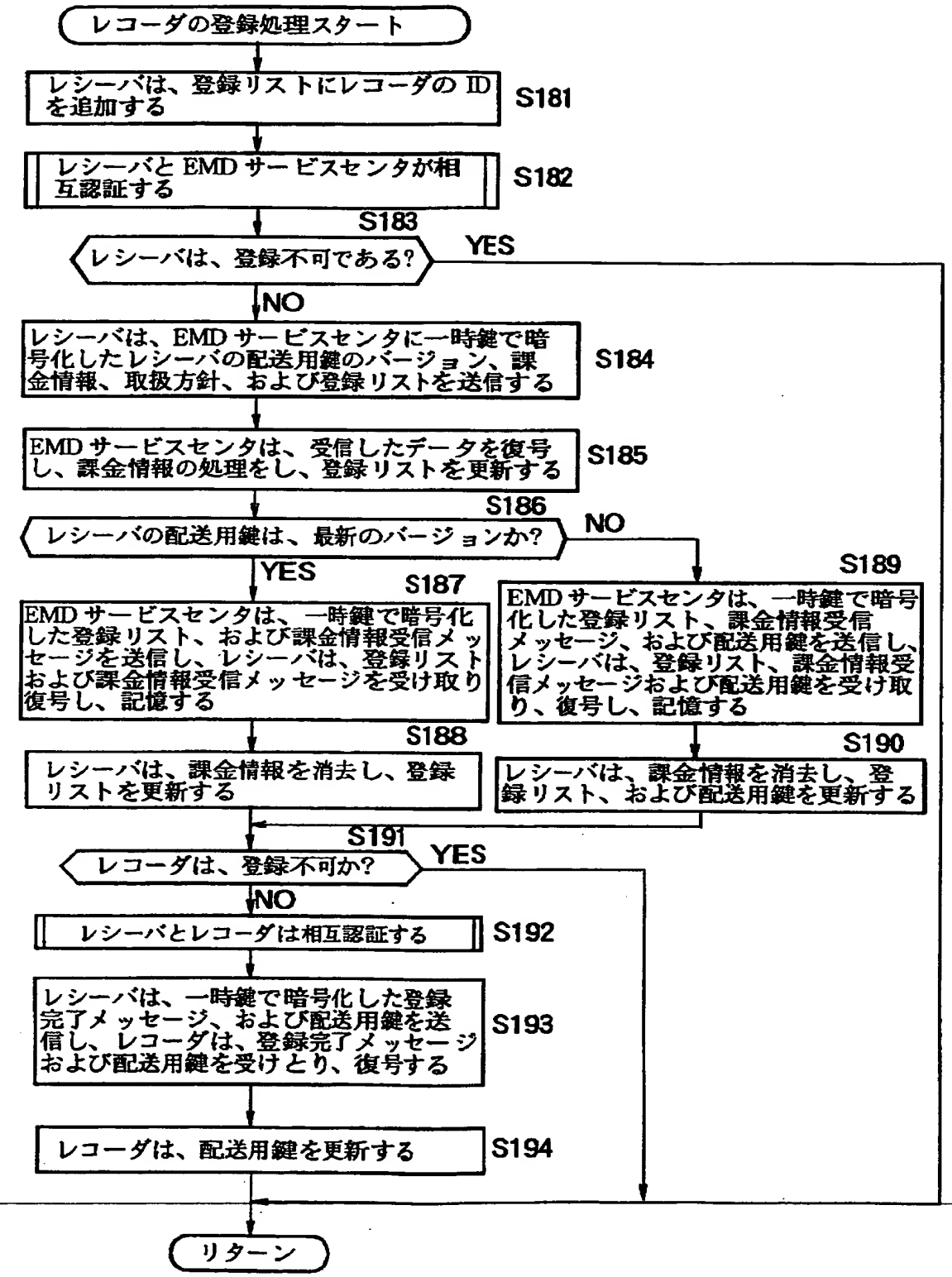
【図５０】


新しいレシーバへのバックアップの読み込み処理スタート
SAMはICカードと相互認証する
S141
ICカードから、暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、読み出す
S142
SAMはEMDサービスセンタと相互認証する
S143
SAMはEMDサービスセンタに暗号化されたSAM内の記憶データと、暗号化されたバックアップ鍵を、送信する
S144
EMDサービスセンタは、秘密鍵でバックアップ鍵を復号する
S145
EMDサービスセンタは、バックアップ鍵で、SAM内の記憶データを、復号する
S146
EMDサービスセンタは、一時鍵で、SAM内の記憶データを、暗号化する
S147
EMDサービスセンタは、SAM内の記憶データを、送信する
S148
SAMは、受信したデータを復号し記憶する
S149
EMDサービスセンタは、古いSAMのIDを登録不可とする
S150
リターン

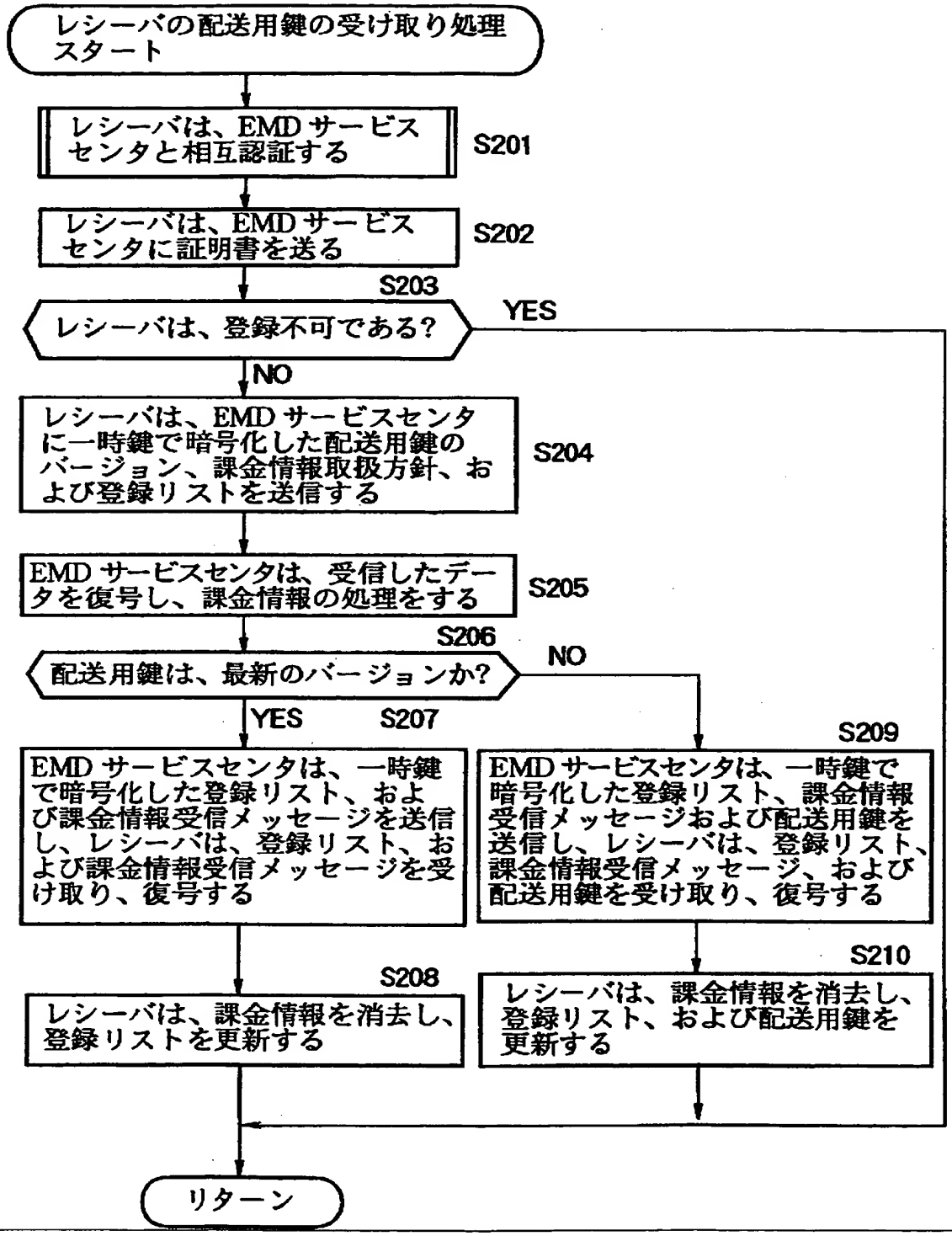
【図５１】


新しいレシーバへのバックアップの読み込み処理スタート
SAMはICカードと相互認証する
S161
ICカードから、暗号化されたSAM内の記憶データ読み出す
S162
SAMはEMDサービスセンタと相互認証する
S163
SAMはEMDサービスセンタに暗号化されたSAM内の記憶データを送信する
S164
EMDサービスセンタは、秘密鍵でSAM内の記憶データを復号する
S165
EMDサービスセンタは、一時鍵で、SAM内の記憶データを、暗号化する
S166
EMDサービスセンタは、SAM内の記憶データを、送信する
S167
SAMは、受信したデータを復号し記憶する
S168
EMDサービスセンタは、古いSAMのIDを登録不可とする
S169
リターン

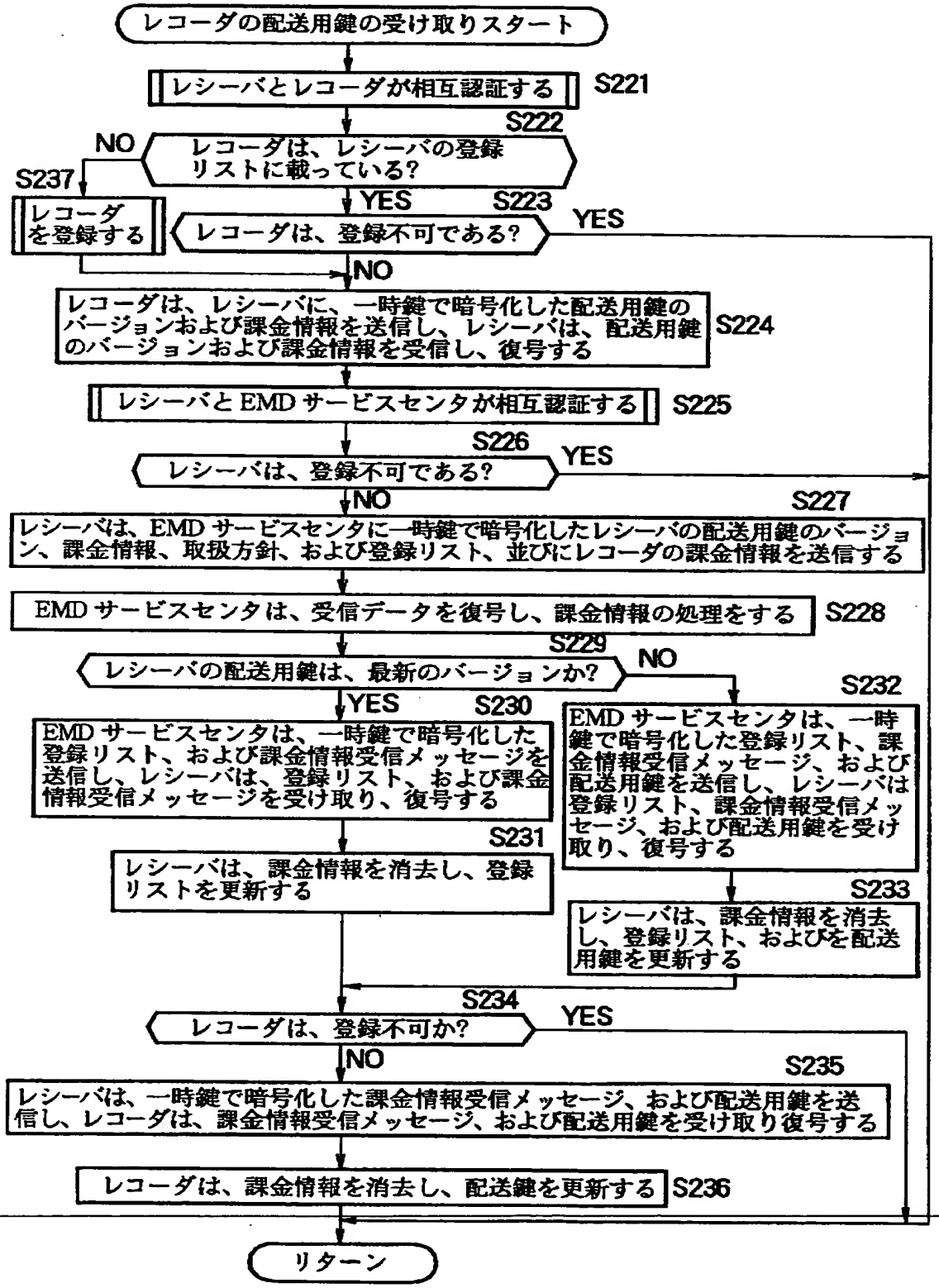
【図５２】


レコーダの登録処理スタート
レシーバは、登録リストにレコーダのIDを追加する
S181
レシーバとEMDサービスセンタが相互認証する
S182
S183
レシーバは、登録不可である?
YES
NO
レシーバは、EMDサービスセンタに一時鍵で暗号化したレシーバの配送用鍵のバージョン、課金情報、取扱方針、および登録リストを送信する
S184
EMDサービスセンタは、受信したデータを復号し、課金情報の処理をし、登録リストを更新する
S185
S186
レシーバの配送用鍵は、最新のバージョンか?
NO
YES
S187
EMDサービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リストおよび課金情報受信メッセージを受け取り復号し、記憶する
S188
レシーバは、課金情報を消去し、登録リストを更新する
S189
EMDサービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージ、および配送用鍵を送信し、レシーバは、登録リスト、課金情報受信メッセージおよび配送用鍵を受け取り、復号し、記憶する
S190
レシーバは、課金情報を消去し、登録リスト、および配送用鍵を更新する
S191
レコーダは、登録不可か?
YES
NO
レシーバとレコーダは相互認証する
S192
レシーバは、一時鍵で暗号化した登録完了メッセージ、および配送用鍵を送信し、レコーダは、登録完了メッセージおよび配送用鍵を受けとり、復号する
S193
レコーダは、配送用鍵を更新する
S194
リターン

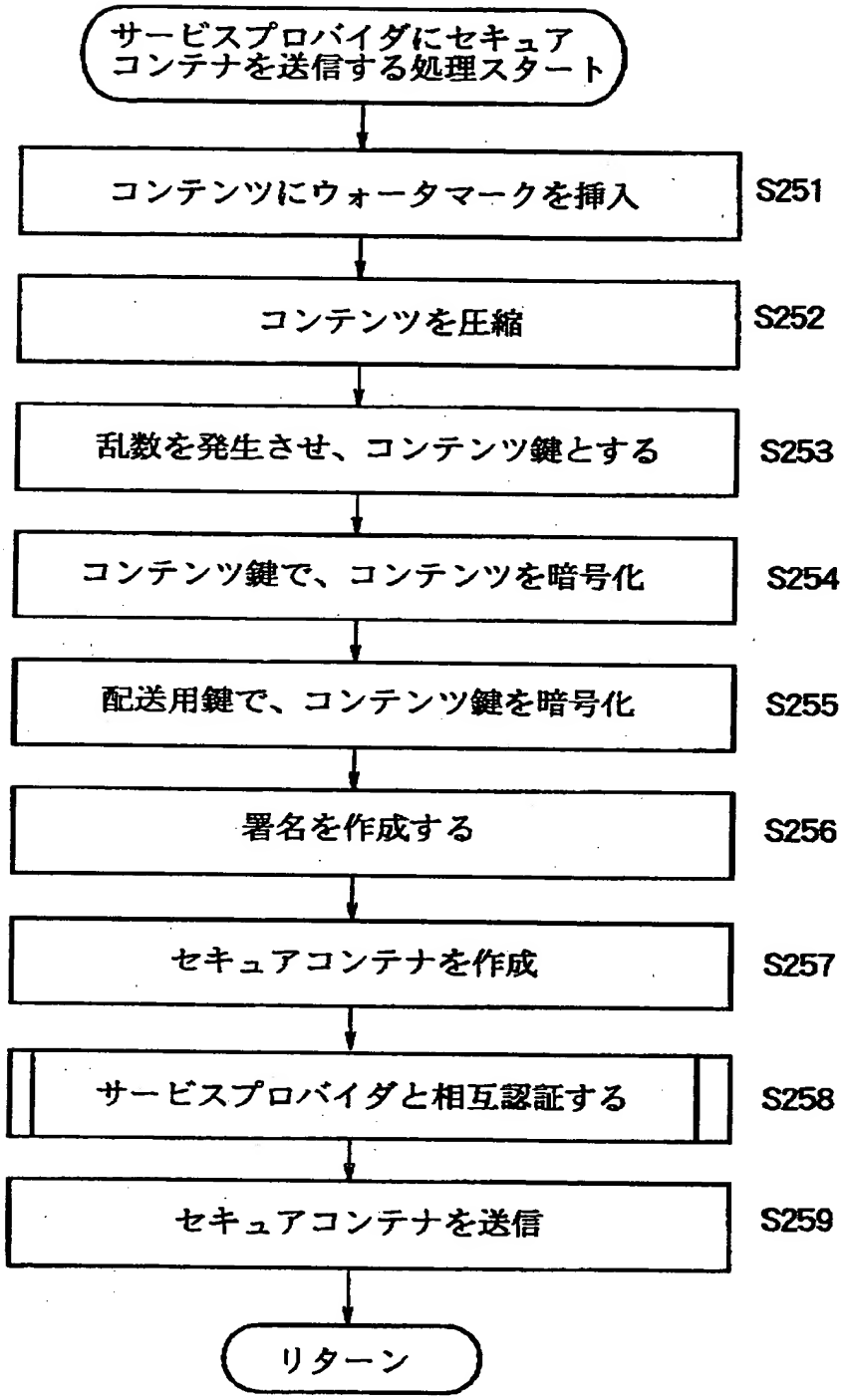
【図５３】


レシーバの配送用鍵の受け取り処理スタート
レシーバは、EMDサービスセンタと相互認証する
S201
レシーバは、EMDサービスセンタに証明書を送る
S202
S203
レシーバは、登録不可である?
YES
NO
レシーバは、EMDサービスセンタに一時鍵で暗号化した配送用鍵のバージョン、課金情報取扱方針、および登録リストを送信する
S204
EMDサービスセンタは、受信したデータを復号し、課金情報の処理をする
S205
S206
配送用鍵は、最新のバージョンか?
NO
YES
S207
S209
EMDサービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リスト、および課金情報受信メッセージを受け取り、復号する
EMDサービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージおよび配送用鍵を送信し、レシーバは、登録リスト、課金情報受信メッセージ、および配送用鍵を受け取り、復号する
S208
S210
レシーバは、課金情報を消去し、登録リストを更新する
レシーバは、課金情報を消去し、登録リスト、および配送用鍵を更新する
リターン

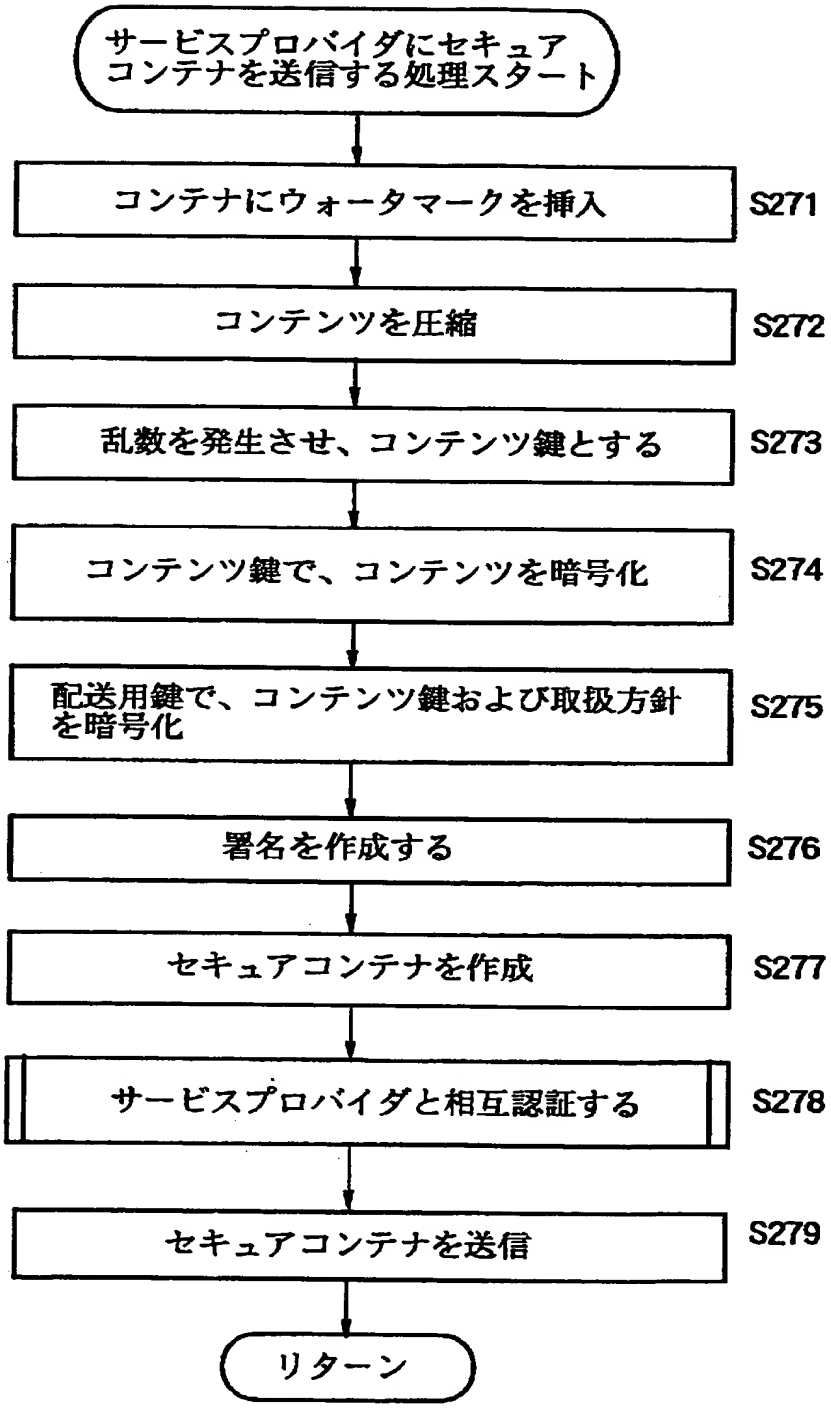
【図５４】


レコーダの配送用鍵の受け取りスタート
レシーバとレコーダが相互認証する
S221
S222
NO
レコーダは、レシーバの登録リストに載っている?
S237
YES
S223
レコーダを登録する
レコーダは、登録不可である?
YES
NO
レコーダは、レシーバに、一時鍵で暗号化した配送用鍵のバージョンおよび課金情報を送信し、レシーバは、配送用鍵のバージョンおよび課金情報を受信し、復号する
S224
レシーバとEMDサービスセンタが相互認証する
S225
S226
レシーバは、登録不可である?
YES
NO
S227
レシーバは、EMDサービスセンタに一時鍵で暗号化したレシーバの配送用鍵のバージョン、課金情報、取扱方針、および登録リスト、並びにレコーダの課金情報を送信する
EMDサービスセンタは、受信データを復号し、課金情報の処理をする
S228
S229
レシーバの配送用鍵は、最新のバージョンか?
NO
S232
YES
S230
EMDサービスセンタは、一時鍵で暗号化した登録リスト、および課金情報受信メッセージを送信し、レシーバは、登録リスト、および課金情報受信メッセージを受け取り、復号する
EMDサービスセンタは、一時鍵で暗号化した登録リスト、課金情報受信メッセージ、および配送用鍵を送信し、レシーバは登録リスト、課金情報受信メッセージ、および配送用鍵を受け取り、復号する
S231
レシーバは、課金情報を消去し、登録リストを更新する
S233
レシーバは、課金情報を消去し、登録リスト、およびを配送用鍵を更新する
S234
レコーダは、登録不可か?
YES
NO
S235
レシーバは、一時鍵で暗号化した課金情報受信メッセージ、および配送用鍵を送信し、レコーダは、課金情報受信メッセージ、および配送用鍵を受け取り復号する
レコーダは、課金情報を消去し、配送鍵を更新する
S236
リターン

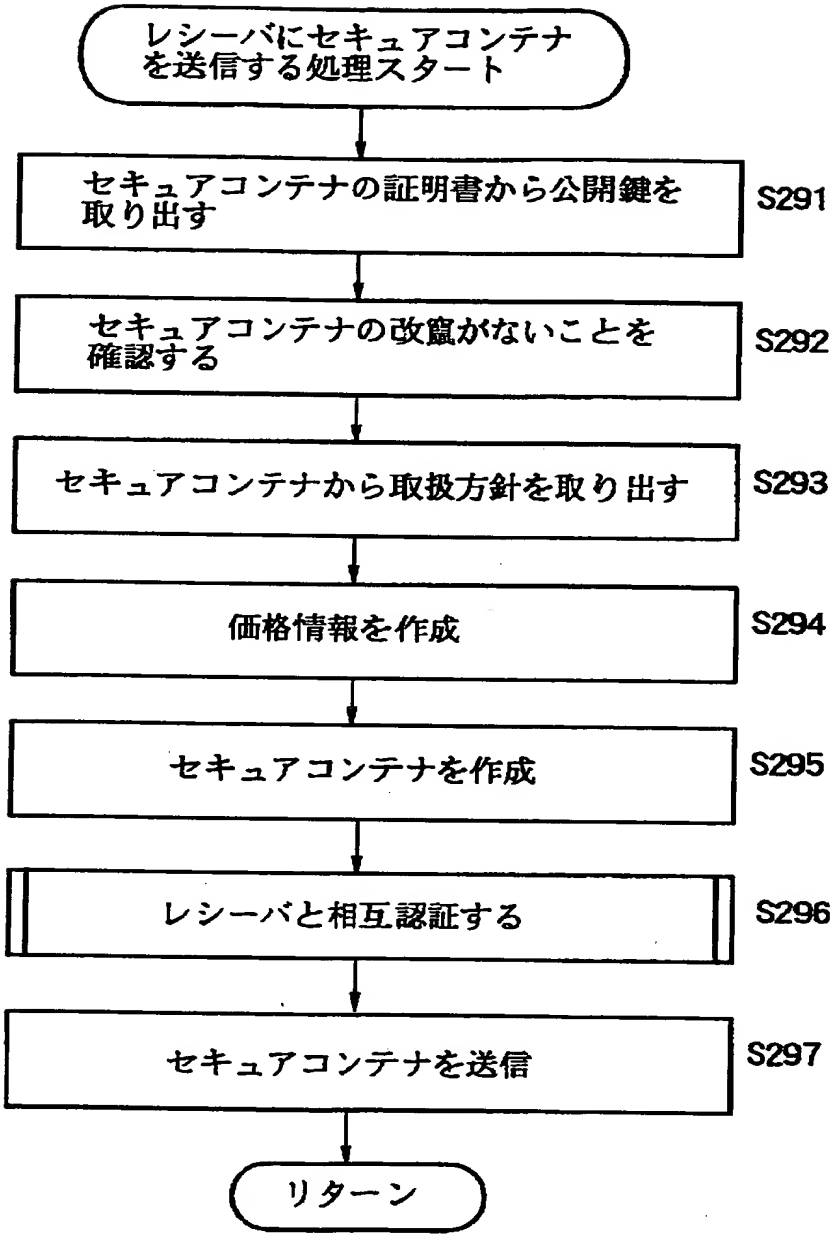
【図５５】


サービスプロバイダにセキュアコンテナを送信する処理スタート
コンテンツにウォータマークを挿入
S251
コンテンツを圧縮
S252
乱数を発生させ、コンテンツ鍵とする
S253
コンテンツ鍵で、コンテンツを暗号化
S254
配送用鍵で、コンテンツ鍵を暗号化
S255
署名を作成する
S256
セキュアコンテナを作成
S257
サービスプロバイダと相互認証する
S258
セキュアコンテナを送信
S259
リターン

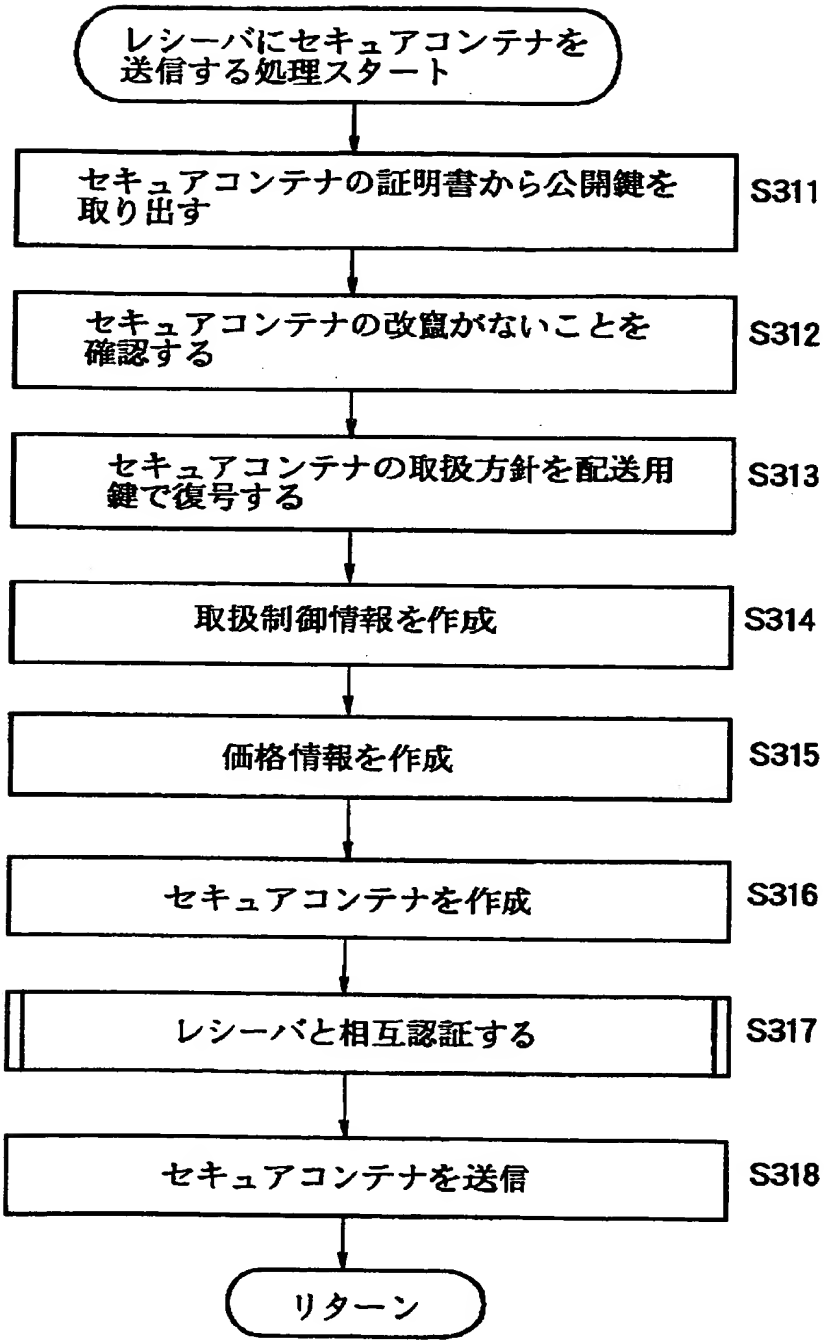
【図５６】


サービスプロバイダにセキュアコンテナを送信する処理スタート
コンテナにウォータマークを挿入
S271
コンテンツを圧縮
S272
乱数を発生させ、コンテンツ鍵とする
S273
コンテンツ鍵で、コンテンツを暗号化
S274
配送用鍵で、コンテンツ鍵および取扱方針を暗号化
S275
署名を作成する
S276
セキュアコンテナを作成
S277
サービスプロバイダと相互認証する
S278
セキュアコンテナを送信
S279
リターン

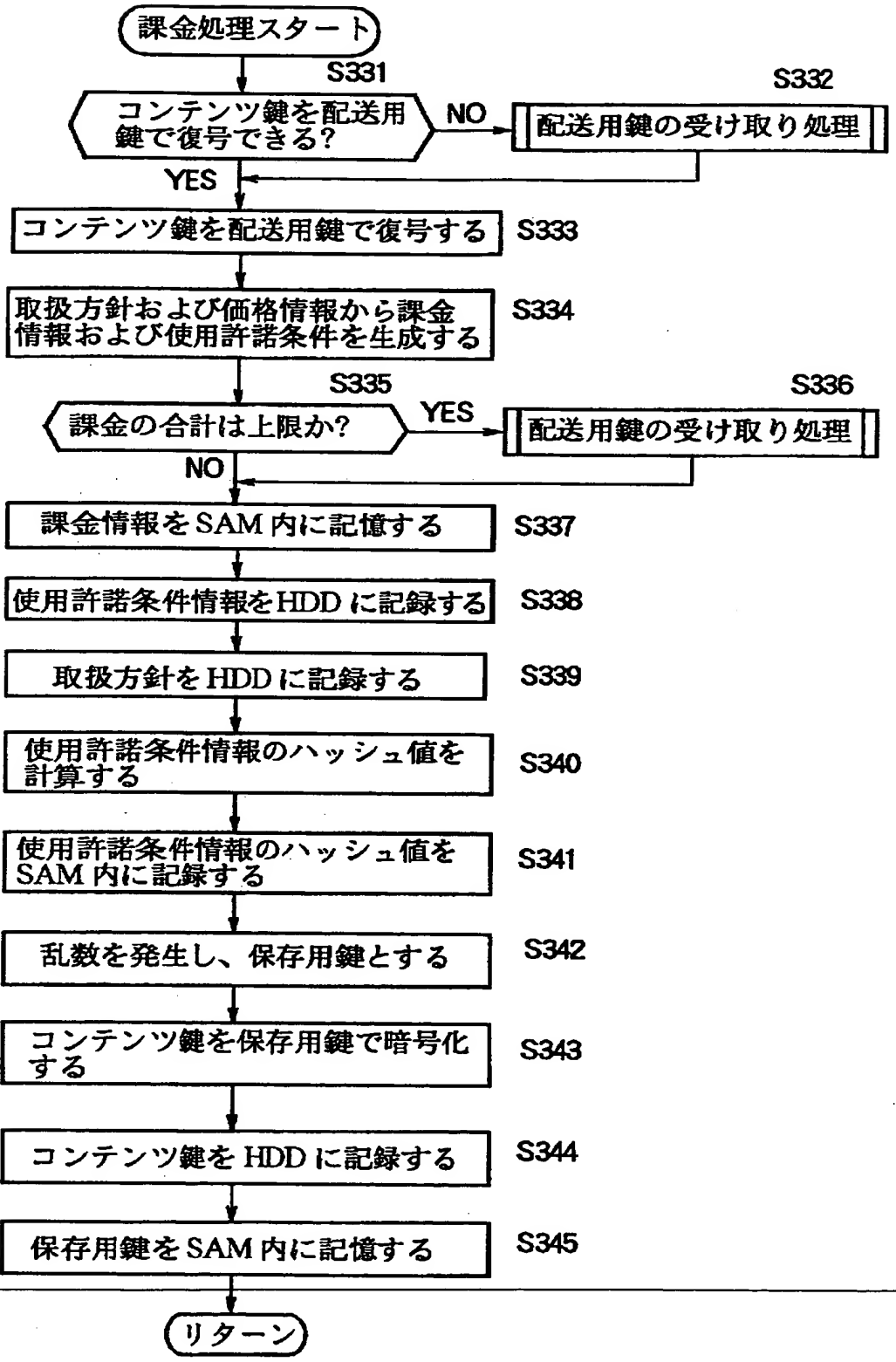
【図５７】


レシーバにセキュアコンテナを送信する処理スタート
セキュアコンテナの証明書から公開鍵を取り出す
S291
セキュアコンテナの改竄がないことを確認する
S292
セキュアコンテナから取扱方針を取り出す
S293
価格情報を作成
S294
セキュアコンテナを作成
S295
レシーバと相互認証する
S296
セキュアコンテナを送信
S297
リターン

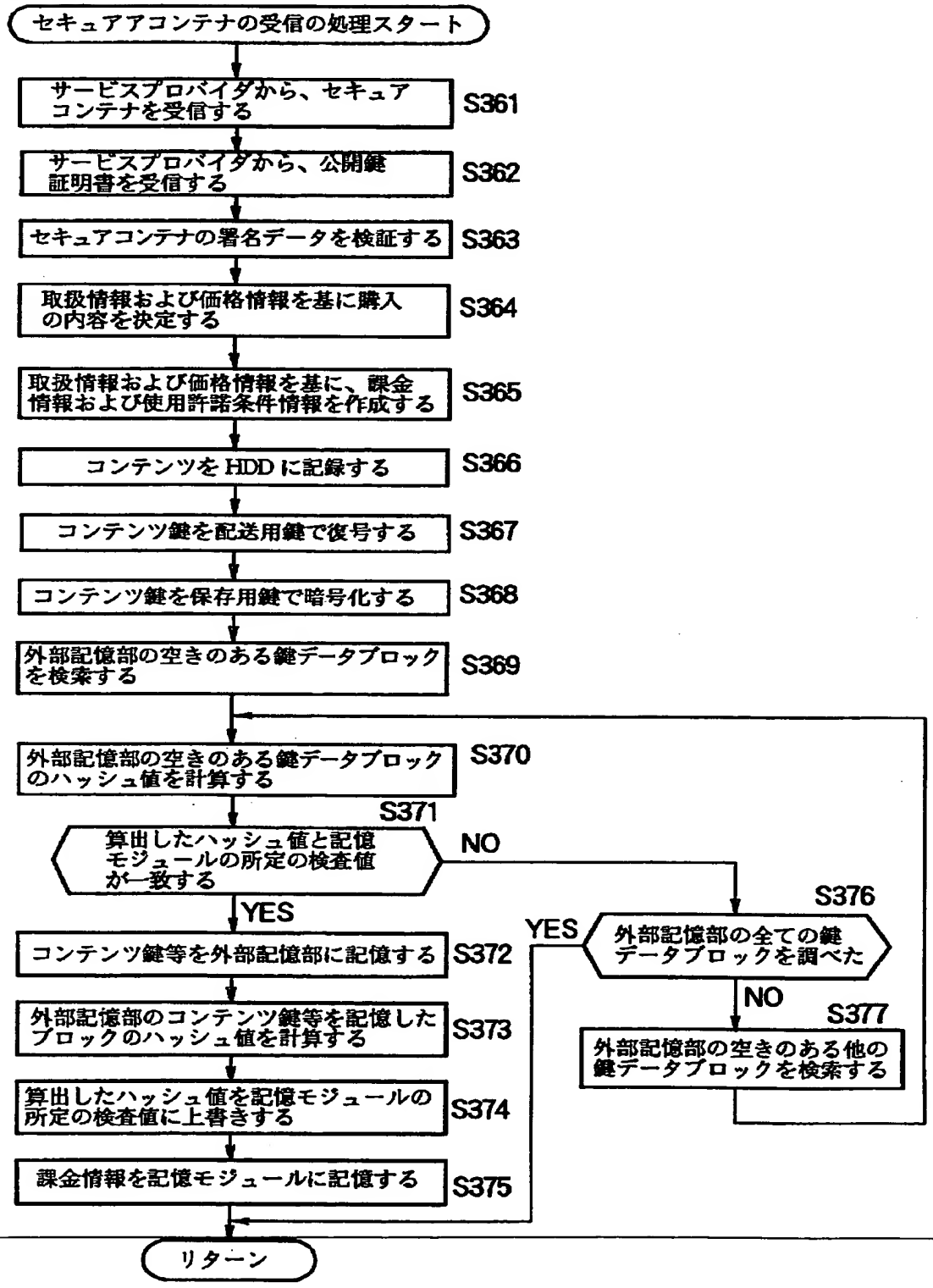
【図５８】


レシーバにセキュアコンテナを送信する処理スタート
セキュアコンテナの証明書から公開鍵を取り出す
S311
セキュアコンテナの改竄がないことを確認する
S312
セキュアコンテナの取扱方針を配送用鍵で復号する
S313
取扱制御情報を作成
S314
価格情報を作成
S315
セキュアコンテナを作成
S316
レシーバと相互認証する
S317
セキュアコンテナを送信
S318
リターン

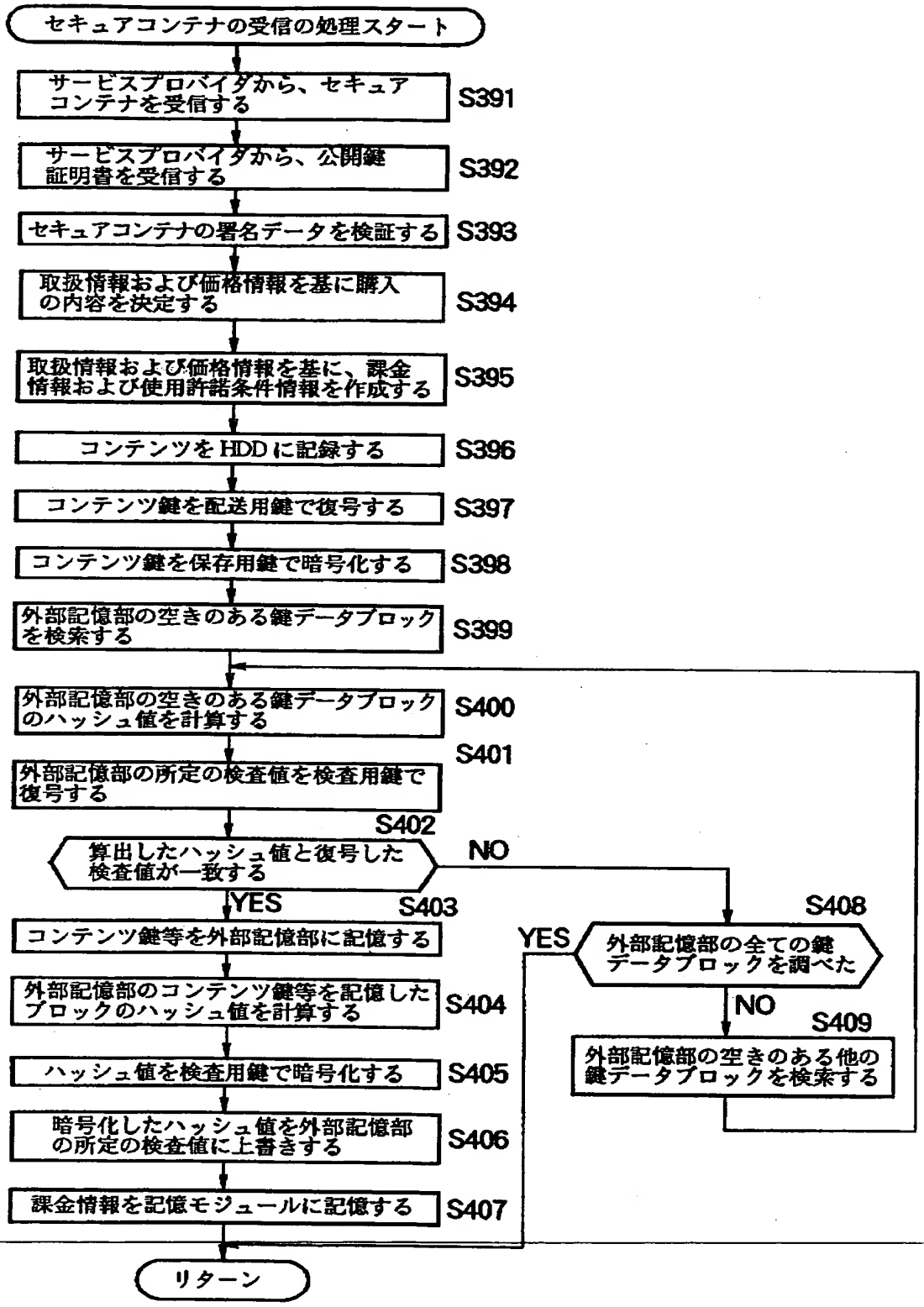
【図５９】


課金処理スタート
S331
コンテンツ鍵を配送用鍵で復号できる?
NO
S332
配送用鍵の受け取り処理
YES
コンテンツ鍵を配送用鍵で復号する
S333
取扱方針および価格情報から課金情報および使用許諾条件を生成する
S334
S335
課金の合計は上限か?
YES
S336
配送用鍵の受け取り処理
NO
課金情報をSAM内に記憶する
S337
使用許諾条件情報をHDDに記録する
S338
取扱方針をHDDに記録する
S339
使用許諾条件情報のハッシュ値を計算する
S340
使用許諾条件情報のハッシュ値をSAM内に記録する
S341
乱数を発生し、保存用鍵とする
S342
コンテンツ鍵を保存用鍵で暗号化する
S343
コンテンツ鍵をHDDに記録する
S344
保存用鍵をSAM内に記憶する
S345
リターン

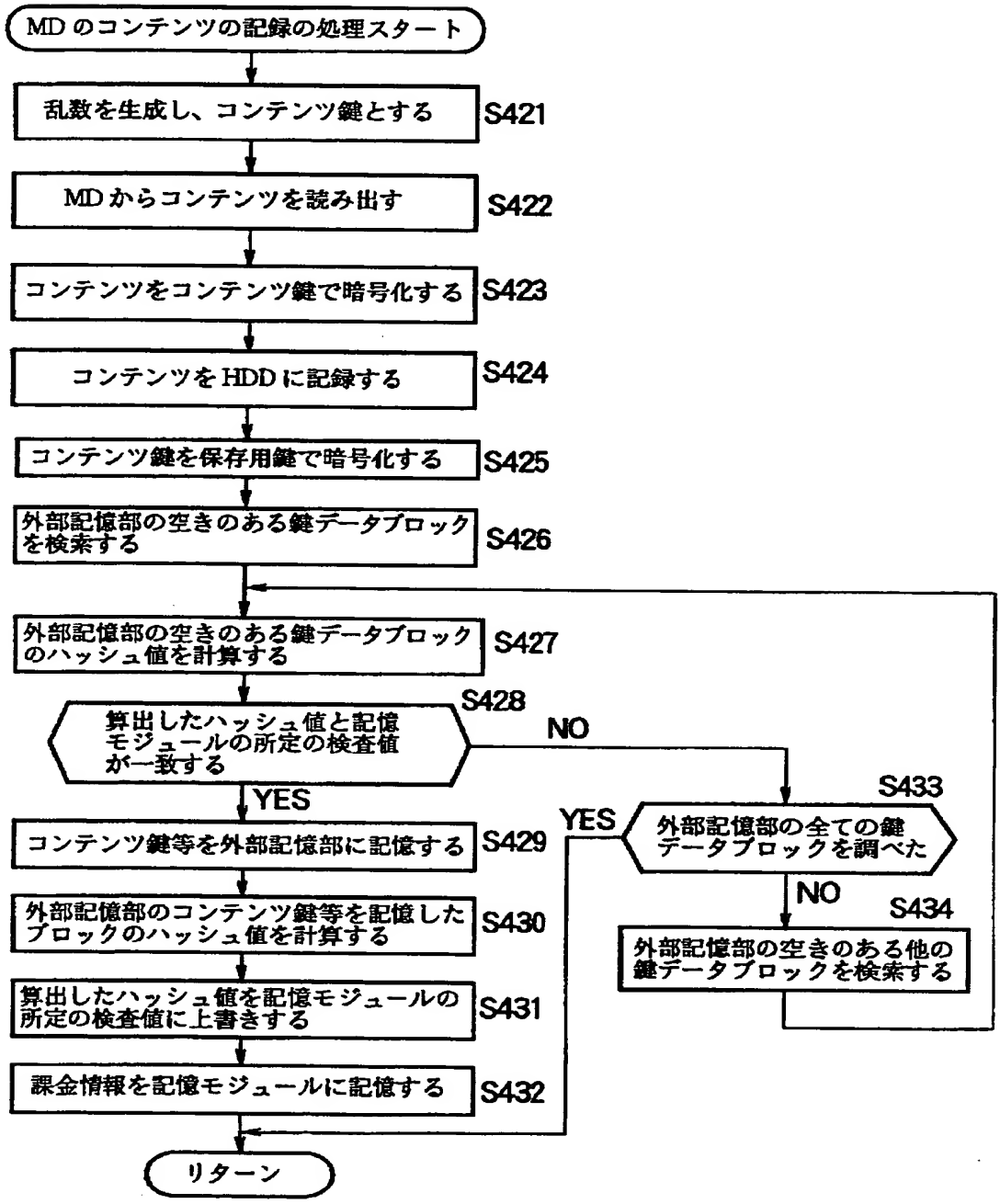
【図６０】


セキュアアコンテナの受信の処理スタート
サービスプロバイダから、セキュアコンテナを受信する
S361
サービスプロバイダから、公開鍵証明書を受信する
S362
セキュアコンテナの署名データを検証する
S363
取扱情報および価格情報を基に購入の内容を決定する
S364
取扱情報および価格情報を基に、課金情報および使用許諾条件情報を作成する
S365
コンテンツをHDDに記録する
S366
コンテンツ鍵を配送用鍵で復号する
S367
コンテンツ鍵を保存用鍵で暗号化する
S368
外部記憶部の空きのある鍵データブロックを検索する
S369
外部記憶部の空きのある鍵データブロックのハッシュ値を計算する
S370
S371
算出したハッシュ値と記憶モジュールの所定の検査値が一致する
NO
YES
S376
外部記憶部の全ての鍵データブロックを調べた
YES
NO
S377
外部記憶部の空きのある他の鍵データブロックを検索する
コンテンツ鍵等を外部記憶部に記憶する
S372
外部記憶部のコンテンツ鍵等を記憶したブロックのハッシュ値を計算する
S373
算出したハッシュ値を記憶モジュールの所定の検査値に上書きする
S374
課金情報を記憶モジュールに記憶する
S375
リターン

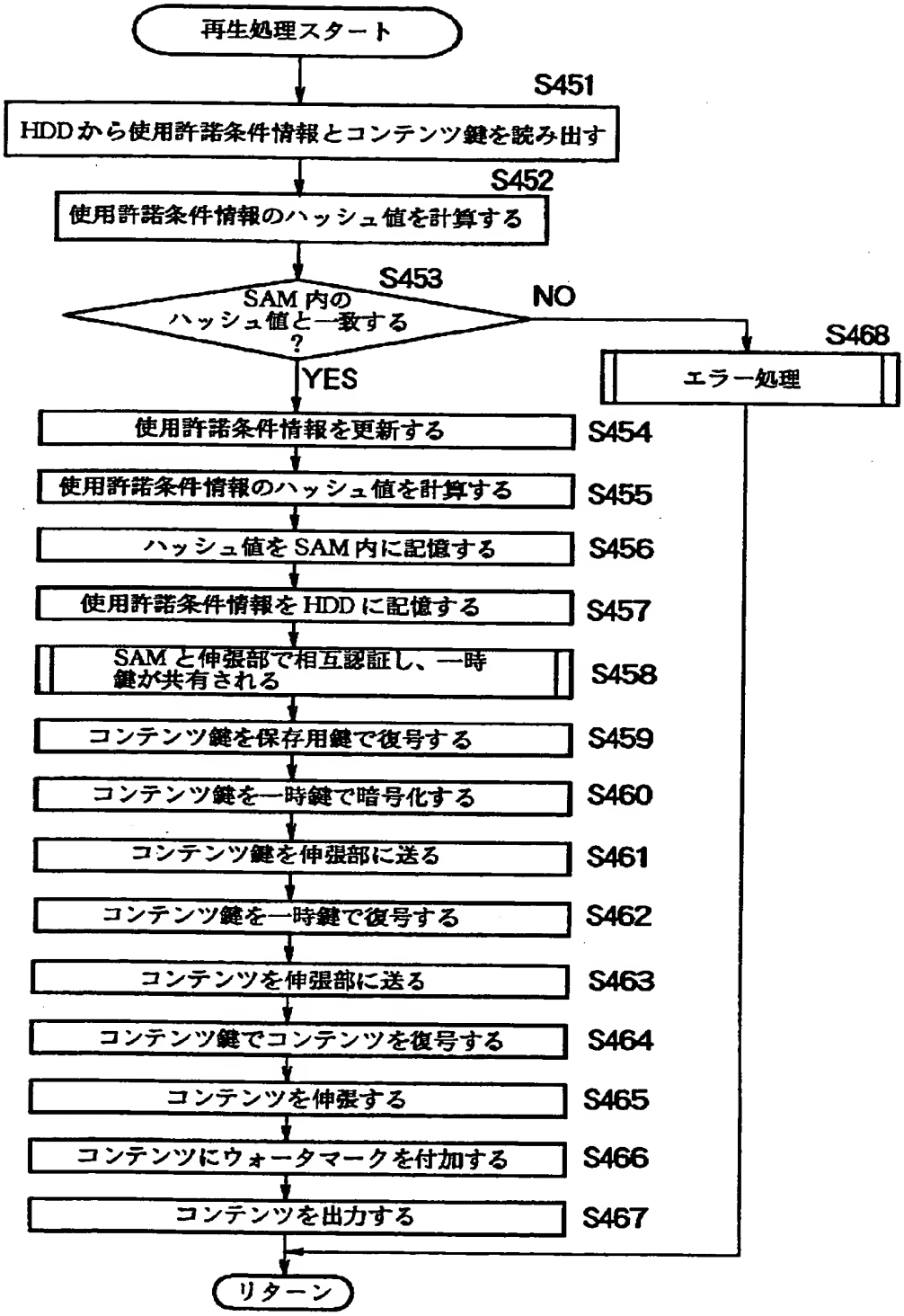
【図６１】


セキュアコンテナの受信の処理スタート
サービスプロバイダから、セキュアコンテナを受信する
S391
サービスプロバイダから、公開鍵証明書を受信する
S392
セキュアコンテナの署名データを検証する
S393
取扱情報および価格情報を基に購入の内容を決定する
S394
取扱情報および価格情報を基に、課金情報および使用許諾条件情報を作成する
S395
コンテンツをHDDに記録する
S396
コンテンツ鍵を配送用鍵で復号する
S397
コンテンツ鍵を保存用鍵で暗号化する
S398
外部記憶部の空きのある鍵データブロックを検索する
S399
外部記憶部の空きのある鍵データブロックのハッシュ値を計算する
S400
外部記憶部の所定の検査値を検査用鍵で復号する
S401
算出したハッシュ値と復号した検査値が一致する
S402
NO
YES
S403
コンテンツ鍵等を外部記憶部に記憶する
外部記憶部のコンテンツ鍵等を記憶したブロックのハッシュ値を計算する
S404
ハッシュ値を検査用鍵で暗号化する
S405
暗号化したハッシュ値を外部記憶部の所定の検査値に上書きする
S406
課金情報を記憶モジュールに記憶する
S407
リターン
S408
YES
外部記憶部の全ての鍵データブロックを調べた
NO
S409
外部記憶部の空きのある他の鍵データブロックを検索する

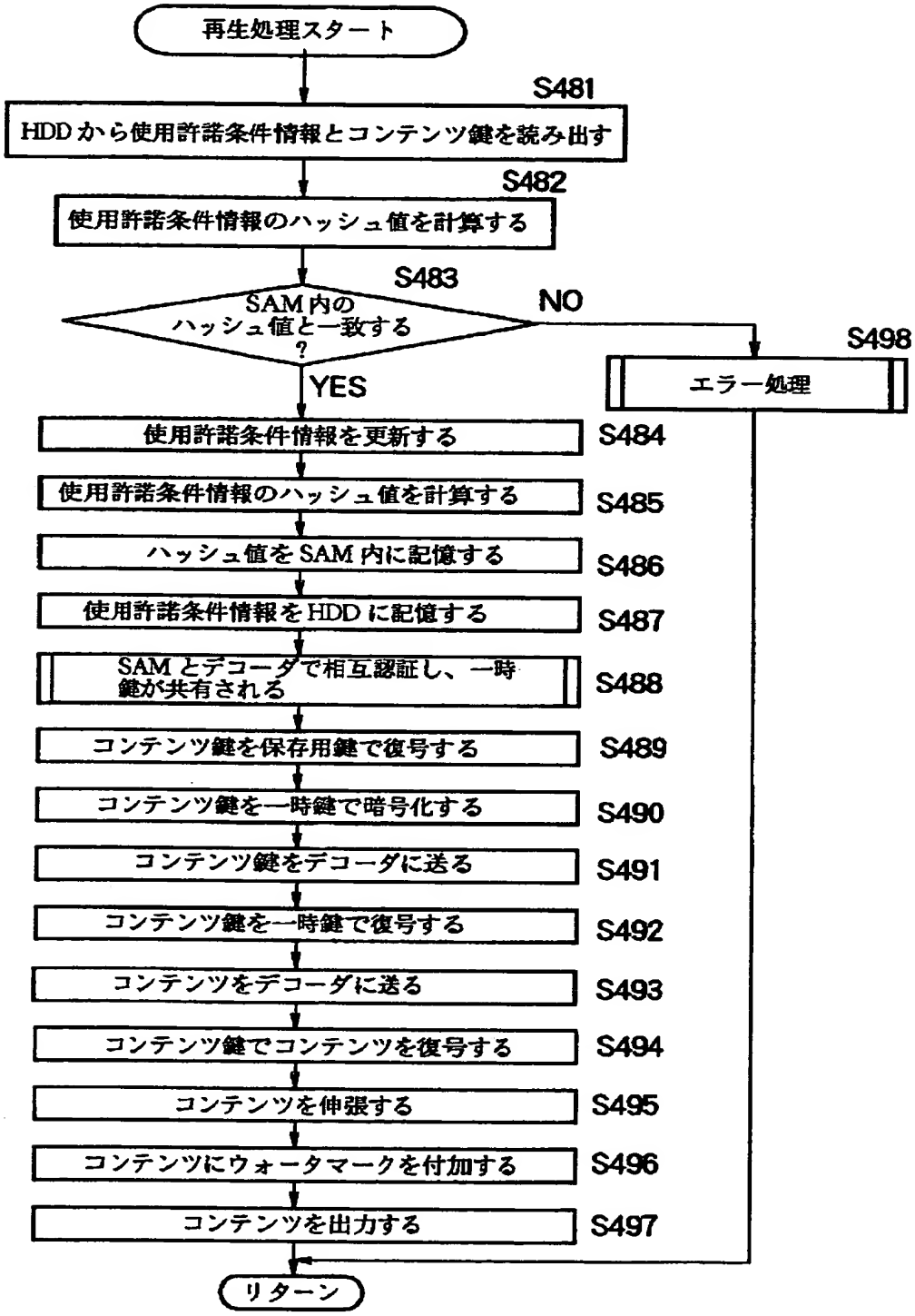
【図６２】


MDのコンテンツの記録の処理スタート
乱数を生成し、コンテンツ鍵とする
S421
MDからコンテンツを読み出す
S422
コンテンツをコンテンツ鍵で暗号化する
S423
コンテンツをHDDに記録する
S424
コンテンツ鍵を保存用鍵で暗号化する
S425
外部記憶部の空きのある鍵データブロックを検索する
S426
外部記憶部の空きのある鍵データブロックのハッシュ値を計算する
S427
S428
算出したハッシュ値と記憶モジュールの所定の検査値が一致する
NO
YES
S433
YES
外部記憶部の全ての鍵データブロックを調べた
NO
S434
外部記憶部の空きのある他の鍵データブロックを検索する
コンテンツ鍵等を外部記憶部に記憶する
S429
外部記憶部のコンテンツ鍵等を記憶したブロックのハッシュ値を計算する
S430
算出したハッシュ値を記憶モジュールの所定の検査値に上書きする
S431
課金情報を記憶モジュールに記憶する
S432
リターン

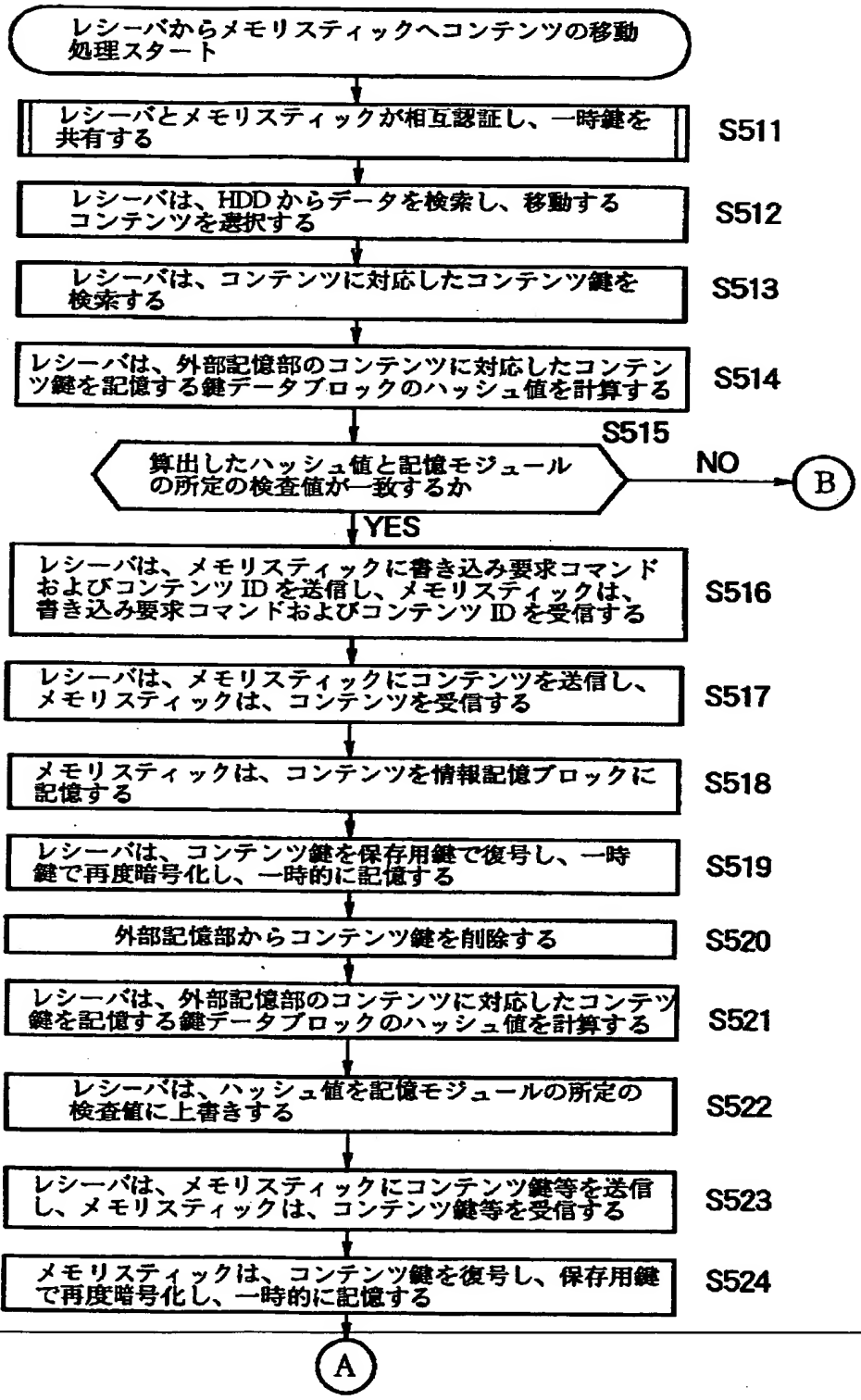
【図６３】


再生処理スタート
S451
HDDから使用許諾条件情報とコンテンツ鍵を読み出す
S452
使用許諾条件情報のハッシュ値を計算する
S453
SAM内のハッシュ値と一致する？
NO
YES
S468
エラー処理
使用許諾条件情報を更新する
S454
使用許諾条件情報のハッシュ値を計算する
S455
ハッシュ値をSAM内に記憶する
S456
使用許諾条件情報をHDDに記憶する
S457
SAMと伸張部で相互認証し、一時鍵が共有される
S458
コンテンツ鍵を保存用鍵で復号する
S459
コンテンツ鍵を一時鍵で暗号化する
S460
コンテンツ鍵を伸張部に送る
S461
コンテンツ鍵を一時鍵で復号する
S462
コンテンツを伸張部に送る
S463
コンテンツ鍵でコンテンツを復号する
S464
コンテンツを伸張する
S465
コンテンツにウォータマークを付加する
S466
コンテンツを出力する
S467
リターン

【図６４】

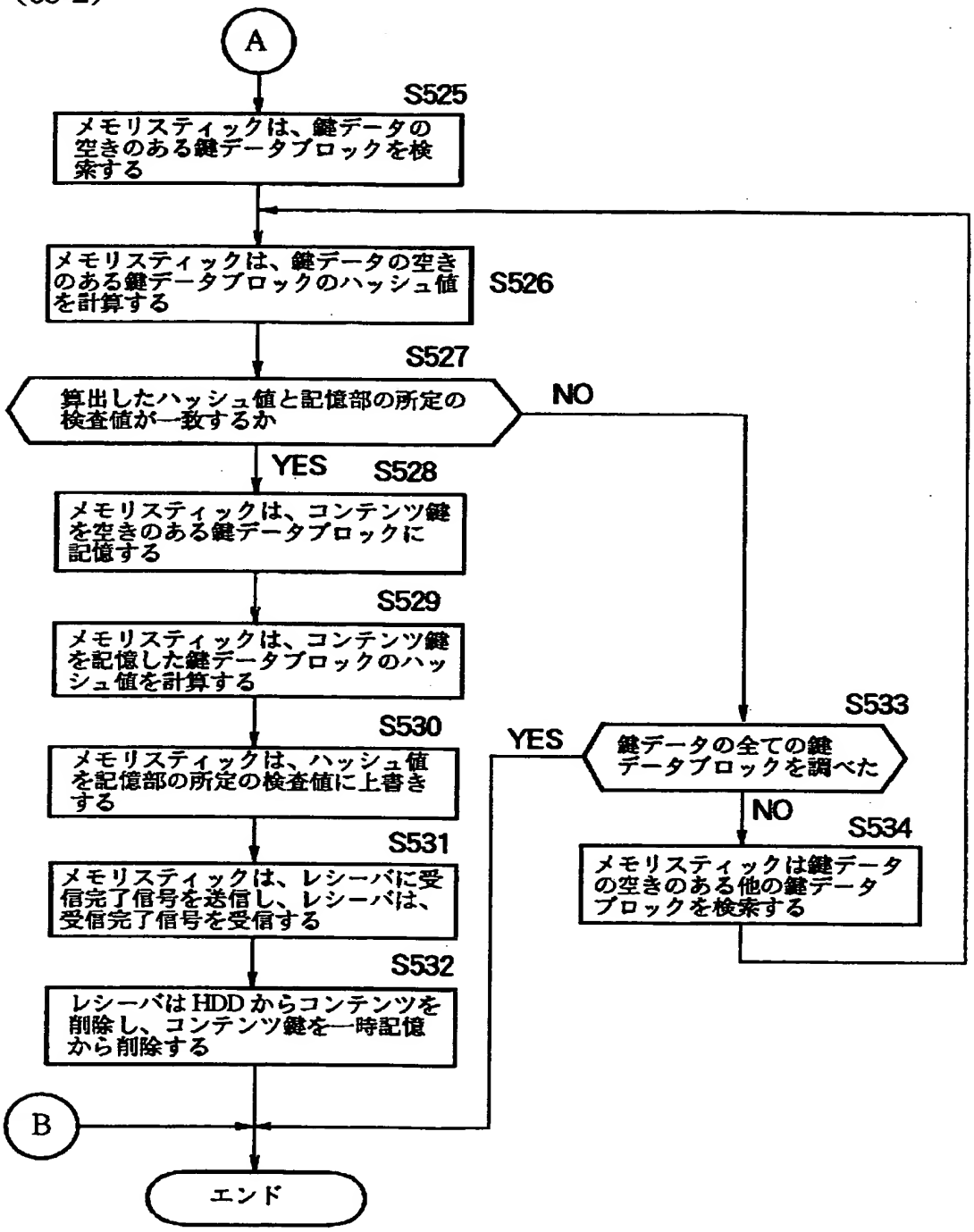

再生処理スタート
S481
HDDから使用許諾条件情報とコンテンツ鍵を読み出す
S482
使用許諾条件情報のハッシュ値を計算する
S483
SAM内のハッシュ値と一致する？
NO
S498
エラー処理
YES
使用許諾条件情報を更新する
S484
使用許諾条件情報のハッシュ値を計算する
S485
ハッシュ値をSAM内に記憶する
S486
使用許諾条件情報をHDDに記憶する
S487
SAMとデコーダで相互認証し、一時鍵が共有される
S488
コンテンツ鍵を保存用鍵で復号する
S489
コンテンツ鍵を一時鍵で暗号化する
S490
コンテンツ鍵をデコーダに送る
S491
コンテンツ鍵を一時鍵で復号する
S492
コンテンツをデコーダに送る
S493
コンテンツ鍵でコンテンツを復号する
S494
コンテンツを伸張する
S495
コンテンツにウォータマークを付加する
S496
コンテンツを出力する
S497
リターン

【図６５】
(65-1)


レシーバからメモリスティックへコンテンツの移動処理スタート
レシーバとメモリスティックが相互認証し、一時鍵を共有する
S511
レシーバは、HDDからデータを検索し、移動するコンテンツを選択する
S512
レシーバは、コンテンツに対応したコンテンツ鍵を検索する
S513
レシーバは、外部記憶部のコンテンツに対応したコンテンツ鍵を記憶する鍵データブロックのハッシュ値を計算する
S514
S515
算出したハッシュ値と記憶モジュールの所定の検査値が一致するか
NO
B
YES
レシーバは、メモリスティックに書き込み要求コマンドおよびコンテンツIDを送信し、メモリスティックは、書き込み要求コマンドおよびコンテンツIDを受信する
S516
レシーバは、メモリスティックにコンテンツを送信し、メモリスティックは、コンテンツを受信する
S517
メモリスティックは、コンテンツを情報記憶ブロックに記憶する
S518
レシーバは、コンテンツ鍵を保存用鍵で復号し、一時鍵で再度暗号化し、一時的に記憶する
S519
外部記憶部からコンテンツ鍵を削除する
S520
レシーバは、外部記憶部のコンテンツに対応したコンテツ鍵を記憶する鍵データブロックのハッシュ値を計算する
S521
レシーバは、ハッシュ値を記憶モジュールの所定の検査値に上書きする
S522
レシーバは、メモリスティックにコンテンツ鍵等を送信し、メモリスティックは、コンテンツ鍵等を受信する
S523
メモリスティックは、コンテンツ鍵を復号し、保存用鍵で再度暗号化し、一時的に記憶する
S524
A

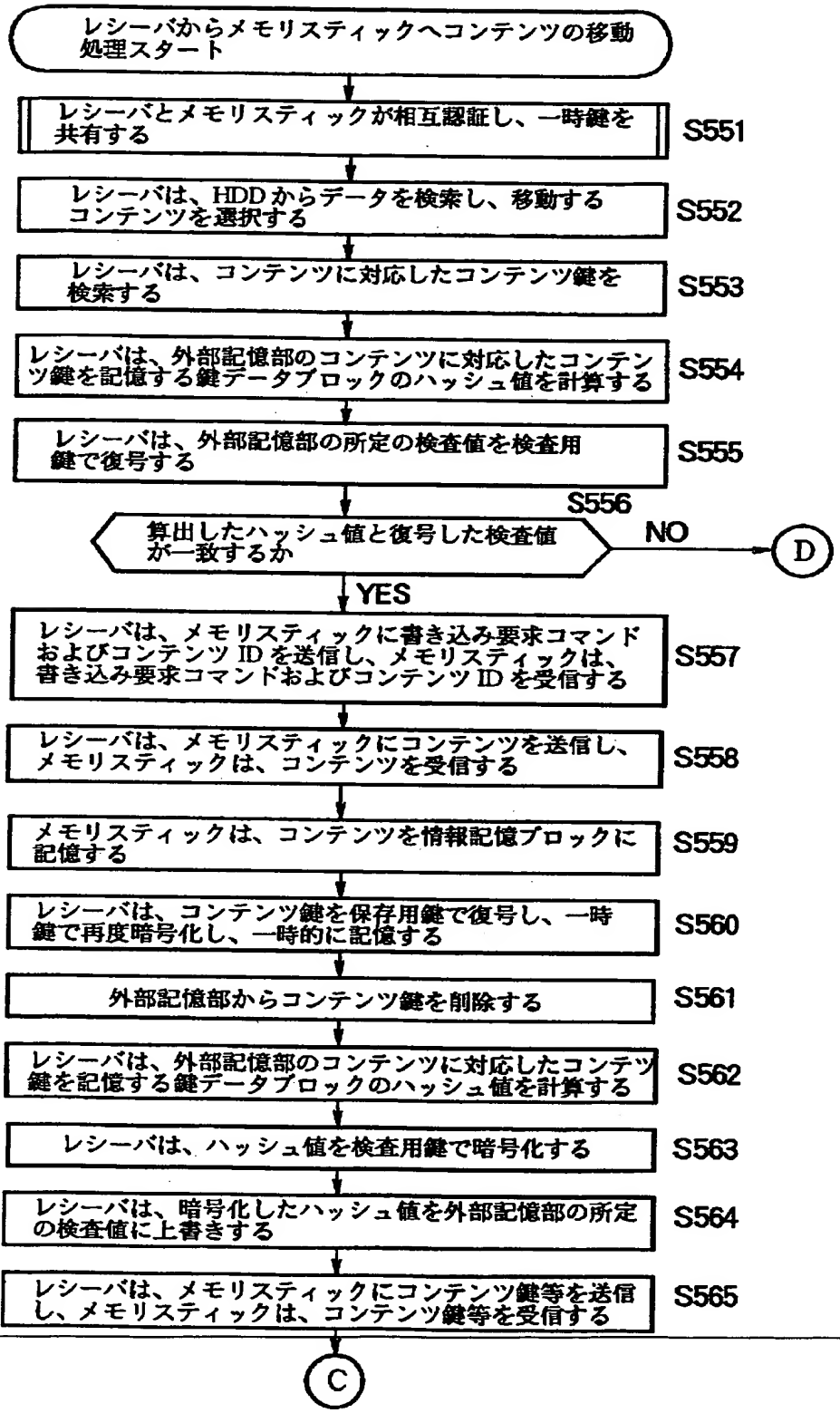
【図６６】

(65-2)


A
S525
メモリスティックは、鍵データの空きのある鍵データブロックを検索する
メモリスティックは、鍵データの空きのある鍵データブロックのハッシュ値を計算する
S526
S527
算出したハッシュ値と記憶部の所定の検査値が一致するか
NO
YES
S528
メモリスティックは、コンテンツ鍵を空きのある鍵データブロックに記憶する
S529
メモリスティックは、コンテンツ鍵を記憶した鍵データブロックのハッシュ値を計算する
S530
メモリスティックは、ハッシュ値を記憶部の所定の検査値に上書きする
S531
メモリスティックは、レシーバに受信完了信号を送信し、レシーバは、受信完了信号を受信する
S532
レシーバはHDDからコンテンツを削除し、コンテンツ鍵を一時記憶から削除する
B
エンド
S533
YES
鍵データの全ての鍵データブロックを調べた
NO
S534
メモリスティックは鍵データの空きのある他の鍵データブロックを検索する

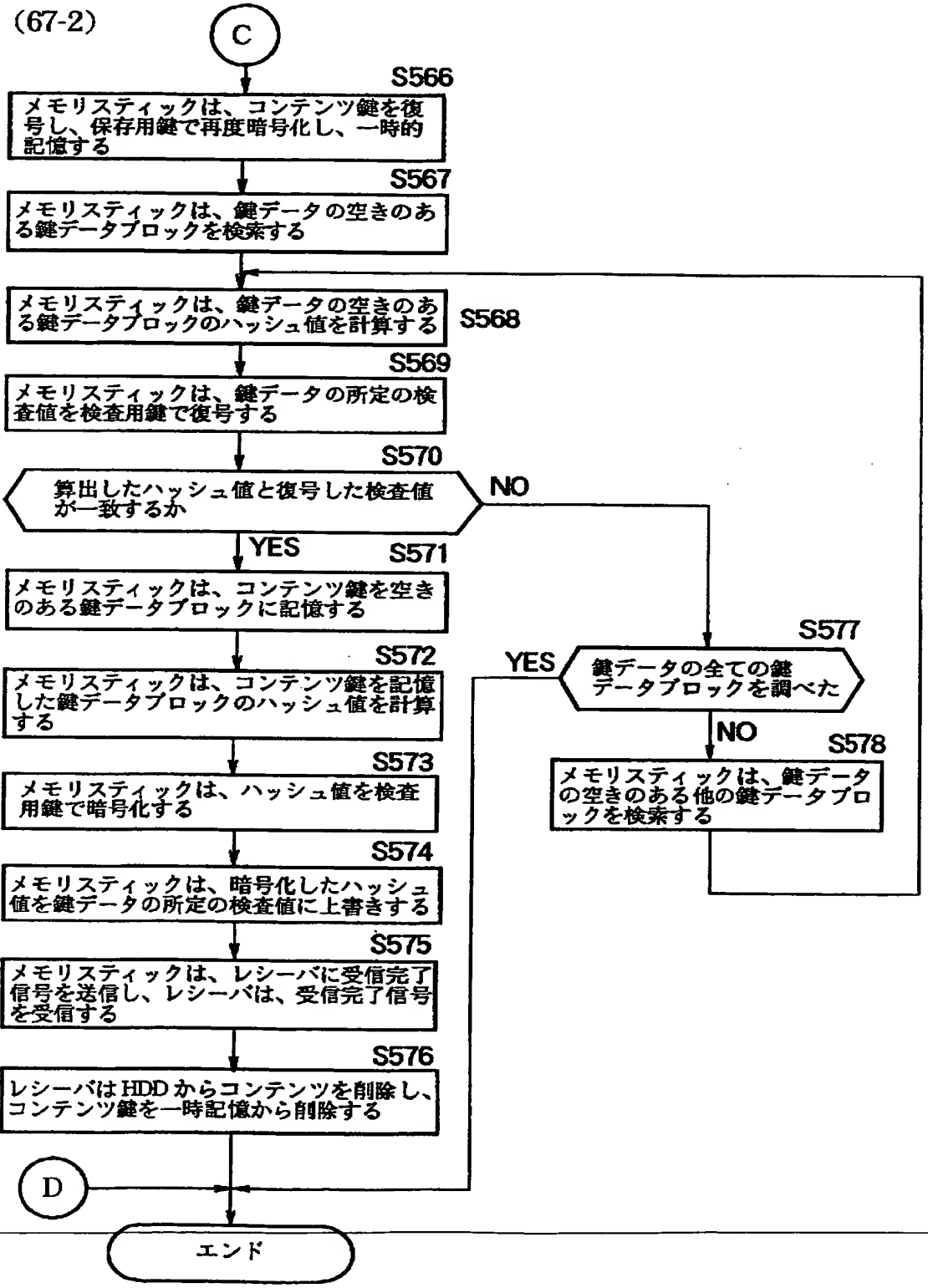
【図６７】

(67-1)


レシーバからメモリスティックへコンテンツの移動処理スタート
レシーバとメモリスティックが相互認証し、一時鍵を共有する
S551
レシーバは、HDDからデータを検索し、移動するコンテンツを選択する
S552
レシーバは、コンテンツに対応したコンテンツ鍵を検索する
S553
レシーバは、外部記憶部のコンテンツに対応したコンテンツ鍵を記憶する鍵データブロックのハッシュ値を計算する
S554
レシーバは、外部記憶部の所定の検査値を検査用鍵で復号する
S555
S556
算出したハッシュ値と復号した検査値が一致するか
NO
D
YES
レシーバは、メモリスティックに書き込み要求コマンドおよびコンテンツIDを送信し、メモリスティックは、書き込み要求コマンドおよびコンテンツIDを受信する
S557
レシーバは、メモリスティックにコンテンツを送信し、メモリスティックは、コンテンツを受信する
S558
メモリスティックは、コンテンツを情報記憶ブロックに記憶する
S559
レシーバは、コンテンツ鍵を保存用鍵で復号し、一時鍵で再度暗号化し、一時的に記憶する
S560
外部記憶部からコンテンツ鍵を削除する
S561
レシーバは、外部記憶部のコンテンツに対応したコンテンツ鍵を記憶する鍵データブロックのハッシュ値を計算する
S562
レシーバは、ハッシュ値を検査用鍵で暗号化する
S563
レシーバは、暗号化したハッシュ値を外部記憶部の所定の検査値に上書きする
S564
レシーバは、メモリスティックにコンテンツ鍵等を送信し、メモリスティックは、コンテンツ鍵等を受信する
S565
C

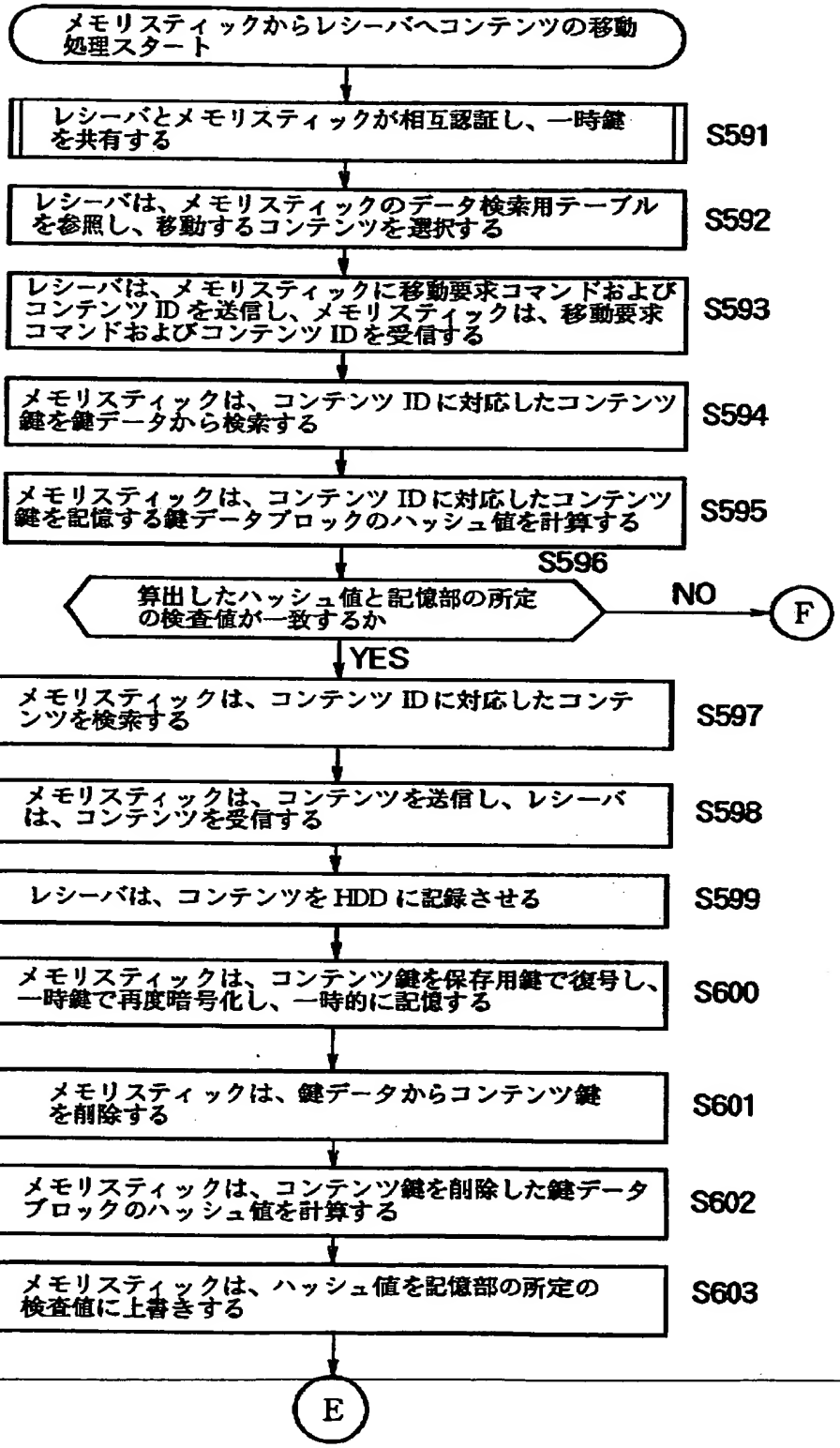
【図６８】

(67-2)


C
S566
メモリスティックは、コンテンツ鍵を復号し、保存用鍵で再度暗号化し、一時的記憶する
S567
メモリスティックは、鍵データの空きのある鍵データブロックを検索する
メモリスティックは、鍵データの空きのある鍵データブロックのハッシュ値を計算する
S568
S569
メモリスティックは、鍵データの所定の検査値を検査用鍵で復号する
S570
算出したハッシュ値と復号した検査値が一致するか
NO
YES
S571
メモリスティックは、コンテンツ鍵を空きのある鍵データブロックに記憶する
S572
メモリスティックは、コンテンツ鍵を記憶した鍵データブロックのハッシュ値を計算する
S573
メモリスティックは、ハッシュ値を検査用鍵で暗号化する
S574
メモリスティックは、暗号化したハッシュ値を鍵データの所定の検査値に上書きする
S575
メモリスティックは、レシーバに受信完了信号を送信し、レシーバは、受信完了信号を受信する
S576
レシーバはHDDからコンテンツを削除し、コンテンツ鍵を一時記憶から削除する
D
エンド
S577
YES
鍵データの全ての鍵データブロックを調べた
NO
S578
メモリスティックは、鍵データの空きのある他の鍵データブロックを検索する

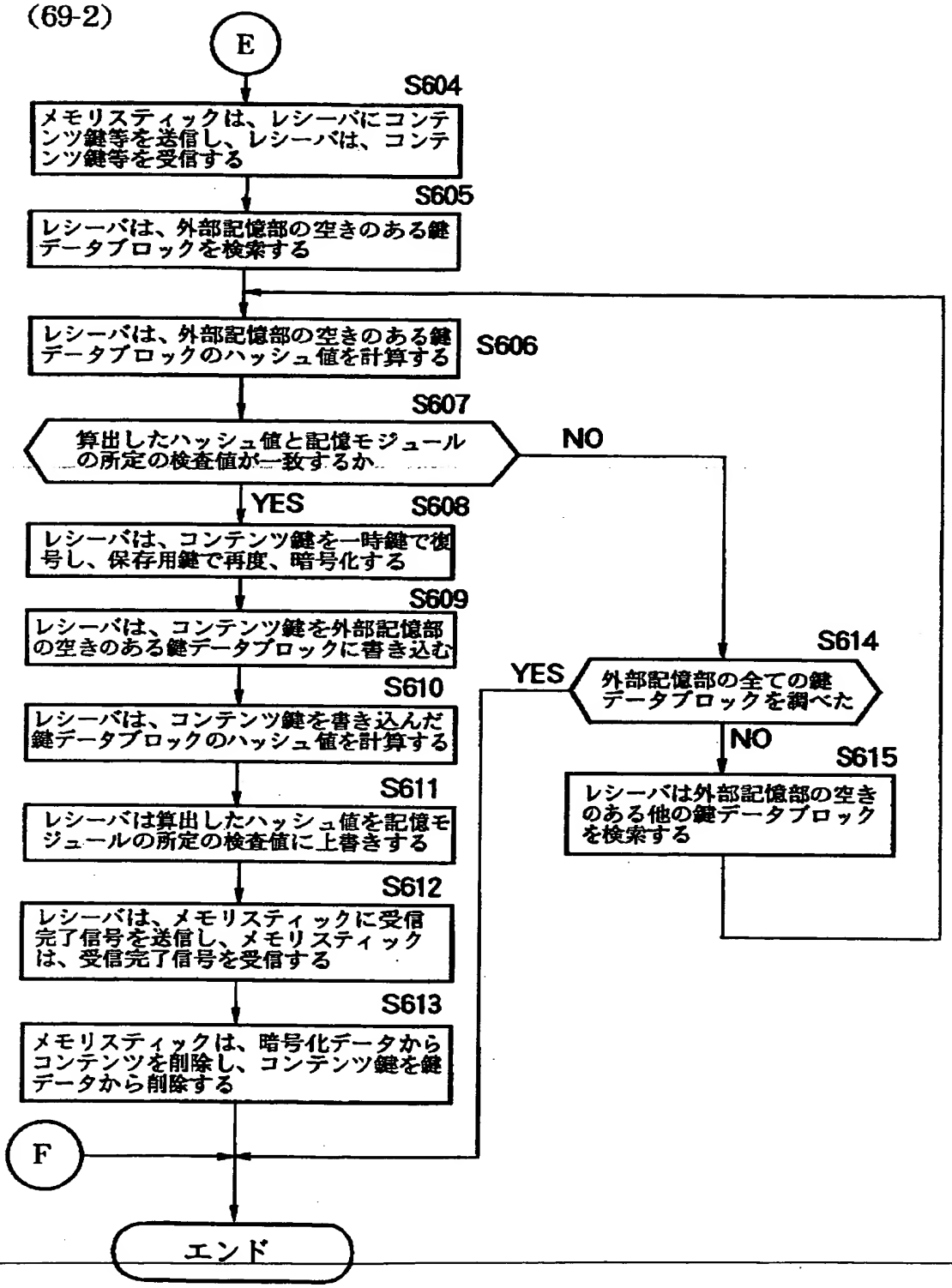
【図６９】

(69-1)

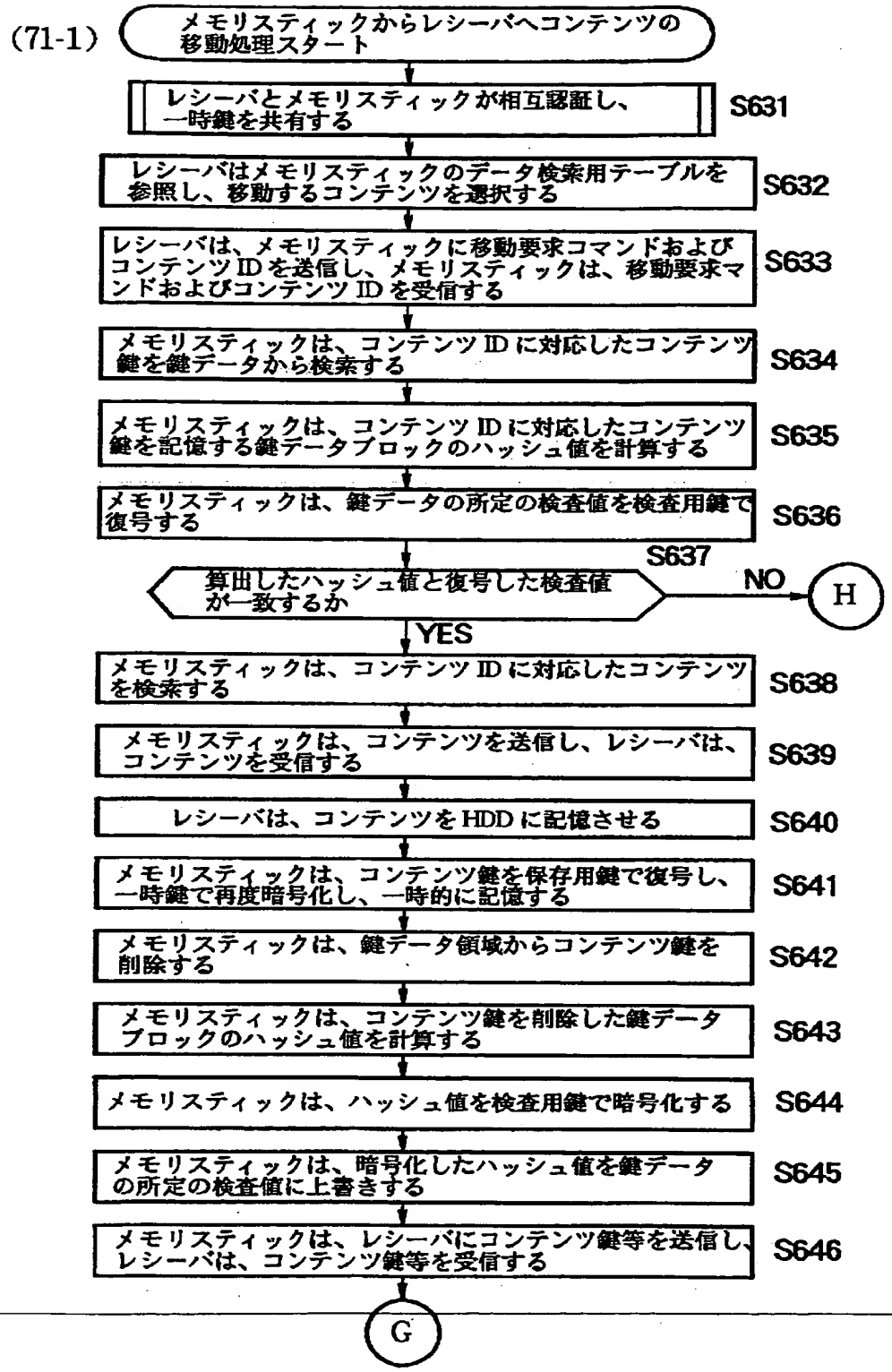

メモリスティックからレシーバへコンテンツの移動処理スタート
レシーバとメモリスティックが相互認証し、一時鍵を共有する
S591
レシーバは、メモリスティックのデータ検索用テーブルを参照し、移動するコンテンツを選択する
S592
レシーバは、メモリスティックに移動要求コマンドおよびコンテンツIDを送信し、メモリスティックは、移動要求コマンドおよびコンテンツIDを受信する
S593
メモリスティックは、コンテンツIDに対応したコンテンツ鍵を鍵データから検索する
S594
メモリスティックは、コンテンツIDに対応したコンテンツ鍵を記憶する鍵データブロックのハッシュ値を計算する
S595
S596
算出したハッシュ値と記憶部の所定の検査値が一致するか
NO
F
YES
メモリスティックは、コンテンツIDに対応したコンテンツを検索する
S597
メモリスティックは、コンテンツを送信し、レシーバは、コンテンツを受信する
S598
レシーバは、コンテンツをHDDに記録させる
S599
メモリスティックは、コンテンツ鍵を保存用鍵で復号し、一時鍵で再度暗号化し、一時的に記憶する
S600
メモリスティックは、鍵データからコンテンツ鍵を削除する
S601
メモリスティックは、コンテンツ鍵を削除した鍵データブロックのハッシュ値を計算する
S602
メモリスティックは、ハッシュ値を記憶部の所定の検査値に上書きする
S603
E

【図７０】

(69-2)

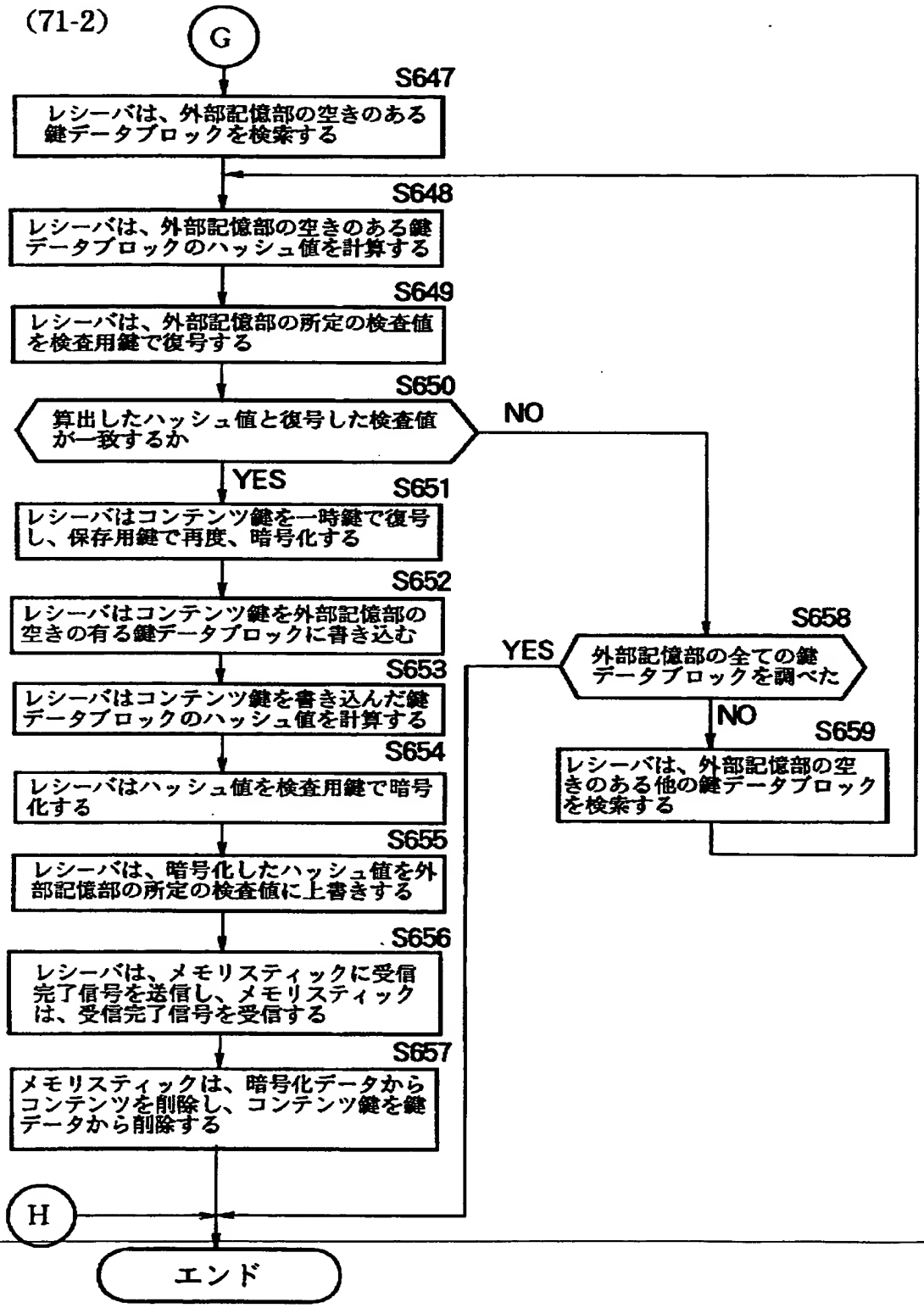

E
S604
メモリスティックは、レシーバにコンテンツ鍵等を送信し、レシーバは、コンテンツ鍵等を受信する
S605
レシーバは、外部記憶部の空きのある鍵データブロックを検索する
レシーバは、外部記憶部の空きのある鍵データブロックのハッシュ値を計算する
S606
S607
算出したハッシュ値と記憶モジュールの所定の検査値が一致するか
NO
YES
S608
レシーバは、コンテンツ鍵を一時鍵で復号し、保存用鍵で再度、暗号化する
S609
レシーバは、コンテンツ鍵を外部記憶部の空きのある鍵データブロックに書き込む
S610
レシーバは、コンテンツ鍵を書き込んだ鍵データブロックのハッシュ値を計算する
S611
レシーバは算出したハッシュ値を記憶モジュールの所定の検査値に上書きする
S612
レシーバは、メモリスティックに受信完了信号を送信し、メモリスティックは、受信完了信号を受信する
S613
メモリスティックは、暗号化データからコンテンツを削除し、コンテンツ鍵を鍵データから削除する
S614
外部記憶部の全ての鍵データブロックを調べた
YES
NO
S615
レシーバは外部記憶部の空きのある他の鍵データブロックを検索する
F
エンド

【図７１】

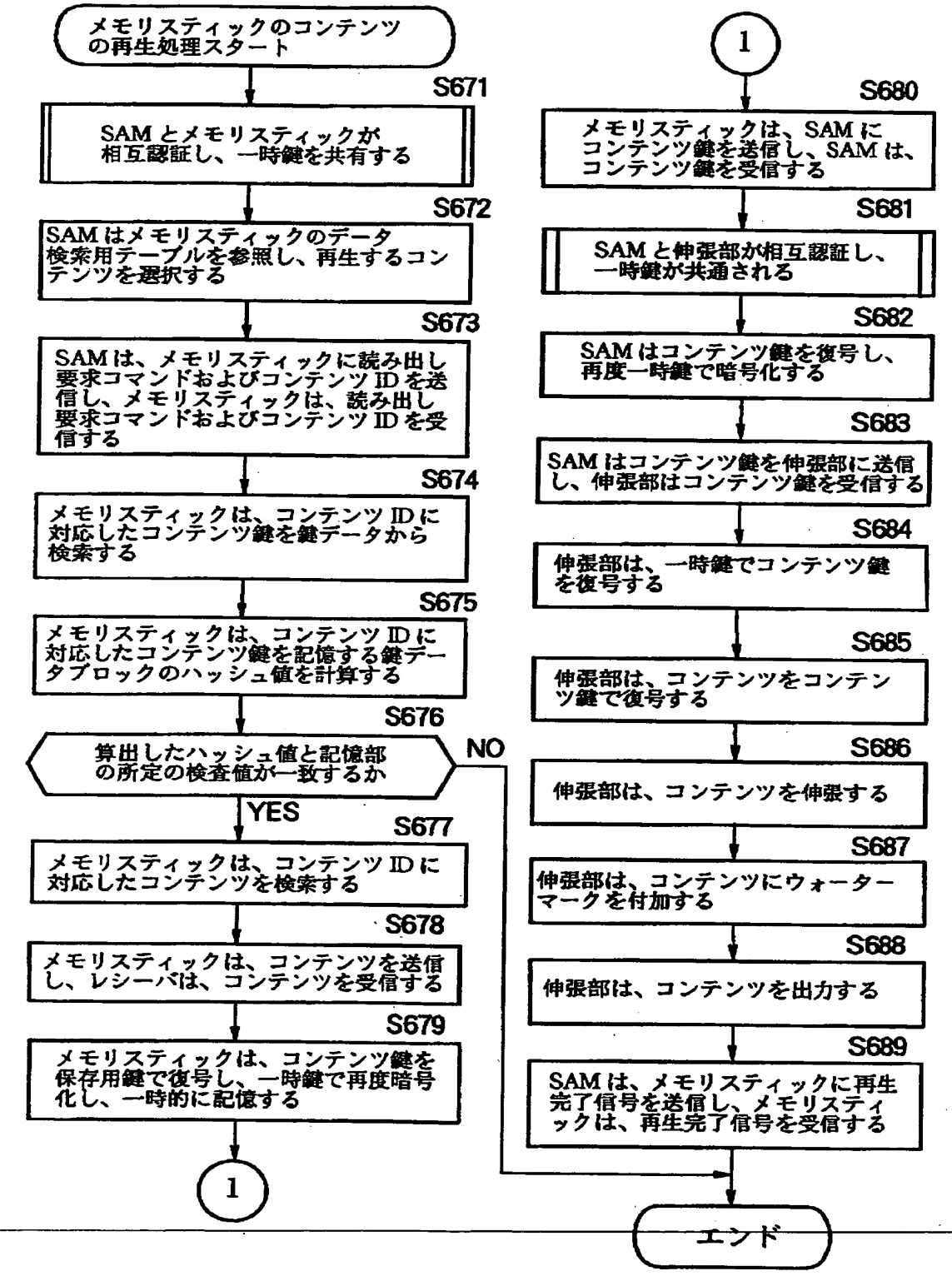

(71-1)
メモリスティックからレシーバへコンテンツの移動処理スタート
レシーバとメモリスティックが相互認証し、一時鍵を共有する
S631
レシーバはメモリスティックのデータ検索用テーブルを参照し、移動するコンテンツを選択する
S632
レシーバは、メモリスティックに移動要求コマンドおよびコンテンツIDを送信し、メモリスティックは、移動要求マンドおよびコンテンツIDを受信する
S633
メモリスティックは、コンテンツIDに対応したコンテンツ鍵を鍵データから検索する
S634
メモリスティックは、コンテンツIDに対応したコンテンツ鍵を記憶する鍵データブロックのハッシュ値を計算する
S635
メモリスティックは、鍵データの所定の検査値を検査用鍵で復号する
S636
S637
算出したハッシュ値と復号した検査値が一致するか
NO
H
YES
メモリスティックは、コンテンツIDに対応したコンテンツを検索する
S638
メモリスティックは、コンテンツを送信し、レシーバは、コンテンツを受信する
S639
レシーバは、コンテンツをHDDに記憶させる
S640
メモリスティックは、コンテンツ鍵を保存用鍵で復号し、一時鍵で再度暗号化し、一時的に記憶する
S641
メモリスティックは、鍵データ領域からコンテンツ鍵を削除する
S642
メモリスティックは、コンテンツ鍵を削除した鍵データブロックのハッシュ値を計算する
S643
メモリスティックは、ハッシュ値を検査用鍵で暗号化する
S644
メモリスティックは、暗号化したハッシュ値を鍵データの所定の検査値に上書きする
S645
メモリスティックは、レシーバにコンテンツ鍵等を送信し、レシーバは、コンテンツ鍵等を受信する
S646
G

【図７２】

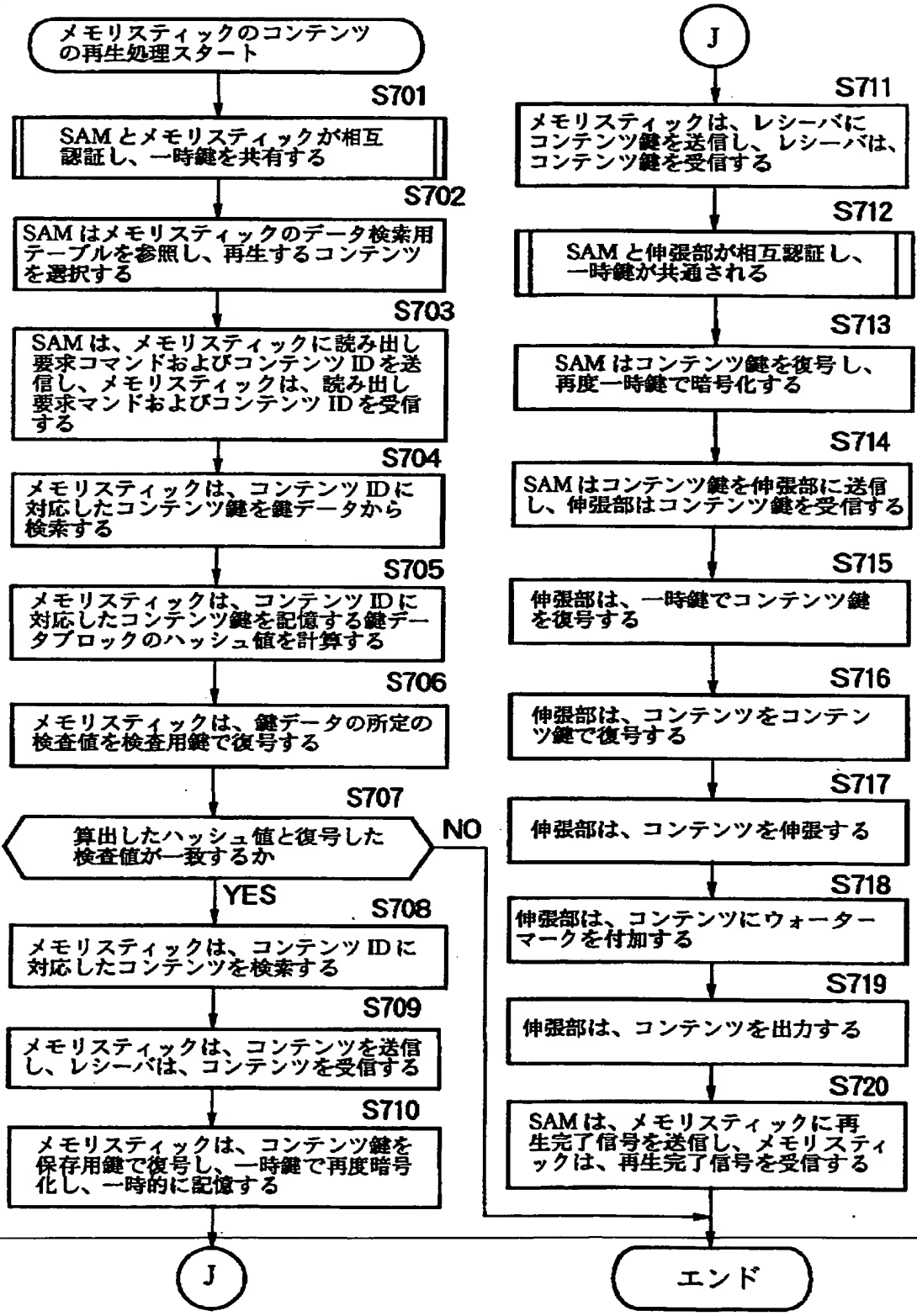
(71-2)


G
S647
レシーバは、外部記憶部の空きのある鍵データブロックを検索する
S648
レシーバは、外部記憶部の空きのある鍵データブロックのハッシュ値を計算する
S649
レシーバは、外部記憶部の所定の検査値を検査用鍵で復号する
S650
算出したハッシュ値と復号した検査値が一致するか
NO
YES
S651
レシーバはコンテンツ鍵を一時鍵で復号し、保存用鍵で再度、暗号化する
S652
レシーバはコンテンツ鍵を外部記憶部の空きの有る鍵データブロックに書き込む
S653
レシーバはコンテンツ鍵を書き込んだ鍵データブロックのハッシュ値を計算する
S654
レシーバはハッシュ値を検査用鍵で暗号化する
S655
レシーバは、暗号化したハッシュ値を外部記憶部の所定の検査値に上書きする
S656
レシーバは、メモリスティックに受信完了信号を送信し、メモリスティックは、受信完了信号を受信する
S657
メモリスティックは、暗号化データからコンテンツを削除し、コンテンツ鍵を鍵データから削除する
S658
外部記憶部の全ての鍵データブロックを調べた
YES
NO
S659
レシーバは、外部記憶部の空きのある他の鍵データブロックを検索する
H
エンド

【図７３】


メモリスティックのコンテンツの再生処理スタート
S671
SAMとメモリスティックが相互認証し、一時鍵を共有する
S672
SAMはメモリスティックのデータ検索用テーブルを参照し、再生するコンテンツを選択する
S673
SAMは、メモリスティックに読み出し要求コマンドおよびコンテンツIDを送信し、メモリスティックは、読み出し要求コマンドおよびコンテンツIDを受信する
S674
メモリスティックは、コンテンツIDに対応したコンテンツ鍵を鍵データから検索する
S675
メモリスティックは、コンテンツIDに対応したコンテンツ鍵を記憶する鍵データブロックのハッシュ値を計算する
S676
算出したハッシュ値と記憶部の所定の検査値が一致するか
NO
YES
S677
メモリスティックは、コンテンツIDに対応したコンテンツを検索する
S678
メモリスティックは、コンテンツを送信し、レシーバは、コンテンツを受信する
S679
メモリスティックは、コンテンツ鍵を保存用鍵で復号し、一時鍵で再度暗号化し、一時的に記憶する
1
1
S680
メモリスティックは、SAMにコンテンツ鍵を送信し、SAMは、コンテンツ鍵を受信する
S681
SAMと伸張部が相互認証し、一時鍵が共通される
S682
SAMはコンテンツ鍵を復号し、再度一時鍵で暗号化する
S683
SAMはコンテンツ鍵を伸張部に送信し、伸張部はコンテンツ鍵を受信する
S684
伸張部は、一時鍵でコンテンツ鍵を復号する
S685
伸張部は、コンテンツをコンテンツ鍵で復号する
S686
伸張部は、コンテンツを伸張する
S687
伸張部は、コンテンツにウォーターマークを付加する
S688
伸張部は、コンテンツを出力する
S689
SAMは、メモリスティックに再生完了信号を送信し、メモリスティックは、再生完了信号を受信する
エンド

【図７４】


メモリスティックのコンテンツの再生処理スタート
S701
SAMとメモリスティックが相互認証し、一時鍵を共有する
S702
SAMはメモリスティックのデータ検索用テーブルを参照し、再生するコンテンツを選択する
S703
SAMは、メモリスティックに読み出し要求コマンドおよびコンテンツIDを送信し、メモリスティックは、読み出し要求マンドおよびコンテンツIDを受信する
S704
メモリスティックは、コンテンツIDに対応したコンテンツ鍵を鍵データから検索する
S705
メモリスティックは、コンテンツIDに対応したコンテンツ鍵を記憶する鍵データブロックのハッシュ値を計算する
S706
メモリスティックは、鍵データの所定の検査値を検査用鍵で復号する
S707
算出したハッシュ値と復号した検査値が一致するか
NO
YES
S708
メモリスティックは、コンテンツIDに対応したコンテンツを検索する
S709
メモリスティックは、コンテンツを送信し、レシーバは、コンテンツを受信する
S710
メモリスティックは、コンテンツ鍵を保存用鍵で復号し、一時鍵で再度暗号化し、一時的に記憶する
J
J
S711
メモリスティックは、レシーバにコンテンツ鍵を送信し、レシーバは、コンテンツ鍵を受信する
S712
SAMと伸張部が相互認証し、一時鍵が共通される
S713
SAMはコンテンツ鍵を復号し、再度一時鍵で暗号化する
S714
SAMはコンテンツ鍵を伸張部に送信し、伸張部はコンテンツ鍵を受信する
S715
伸張部は、一時鍵でコンテンツ鍵を復号する
S716
伸張部は、コンテンツをコンテンツ鍵で復号する
S717
伸張部は、コンテンツを伸張する
S718
伸張部は、コンテンツにウォーターマークを付加する
S719
伸張部は、コンテンツを出力する
S720
SAMは、メモリスティックに再生完了信号を送信し、メモリスティックは、再生完了信号を受信する
エンド

【書類名】　　要約書

【要約】

【課題】　情報の利用内容を示す情報の書き換えを検知する。

【解決手段】　課金処理モジュール７２は、情報の使用の許諾条件を示す情報を生成し、復号／暗号化モジュール７４は、許諾条件を示す情報の認証情報を生成し、記憶モジュール７３は、認証情報を記憶する。

【選択図】　　図１０

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000002185
【住所又は居所】　東京都品川区北品川６丁目７番３５号
【氏名又は名称】　ソニー株式会社
【代理人】　申請人
【識別番号】　100082131
【住所又は居所】　東京都新宿区西新宿７丁目５番８号　ＧＯＷＡ西新宿ビル６Ｆ　稲本国際特許事務所
【氏名又は名称】　稲本　義雄

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
　［変更理由］　新規登録
　　住　所　　東京都品川区北品川６丁目７番３５号
　　氏　名　　ソニー株式会社